

# Digital nets with infinite digit expansions and construction of folded digital nets for quasi-Monte Carlo integration\*

Takashi Goda<sup>†</sup>, Kosuke Suzuki<sup>‡</sup>, Takehito Yoshiki<sup>§</sup>

July 27, 2015

## Abstract

In this paper we study quasi-Monte Carlo integration of smooth functions using digital nets. We fold digital nets over  $\mathbb{Z}_b$  by means of the  $b$ -adic tent transformation, which has recently been introduced by the authors, and employ such *folded digital nets* as quadrature points. We first analyze the worst-case error of quasi-Monte Carlo rules using folded digital nets in reproducing kernel Hilbert spaces. Here we need to permit digital nets with “infinite digit expansions”, which are beyond the scope of the classical definition of digital nets. We overcome this issue by considering the infinite product of cyclic groups and the characters on it. We then give an explicit means of constructing good folded digital nets as follows: we use higher order polynomial lattice point sets for digital nets and show that the component-by-component construction can find good *folded higher order polynomial lattice rules* that achieve the optimal convergence rate of the worst-case error in certain Sobolev spaces of smoothness of arbitrarily high order.

**Keywords:** Quasi-Monte Carlo, numerical integration, tent transformation, folded digital nets, higher order polynomial lattice rules

**MSC classifications:** 65C05, 65D30, 65D32

## 1 Introduction

Quasi-Monte Carlo (QMC) integration of a real-valued function  $f$  defined over the  $s$ -dimensional unit cube is given by

$$Q(f; P) := \frac{1}{|P|} \sum_{\mathbf{x} \in P} f(\mathbf{x}),$$

---

\*The works of the second and third authors were supported by the Program for Leading Graduate Schools, MEXT, Japan.

<sup>†</sup>Graduate School of Engineering, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656 ([goda@frcer.t.u-tokyo.ac.jp](mailto:goda@frcer.t.u-tokyo.ac.jp)).

<sup>‡</sup>Graduate School of Mathematical Sciences, The University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo 153-8914 ([ksuzuki@ms.u-tokyo.ac.jp](mailto:ksuzuki@ms.u-tokyo.ac.jp)), JSPS research fellow.

<sup>§</sup>Graduate School of Mathematical Sciences, The University of Tokyo, 3-8-1 Komaba, Meguro-ku, Tokyo 153-8914 ([yosiki@ms.u-tokyo.ac.jp](mailto:yosiki@ms.u-tokyo.ac.jp)).

where  $P \subset [0, 1]^s$  is a point set and  $|P|$  denotes the cardinality of  $P$ , to approximate the integral

$$I(f) := \int_{[0,1]^s} f(\mathbf{x}) \, d\mathbf{x},$$

as accurately as possible. As one of the main families of QMC point sets, digital nets and sequences have been extensively studied in the literature, see for instance [8, 16]. We shall discuss the definition of digital nets in Subsection 2.3. There have been many good explicit constructions of digital nets and sequences, including those proposed by Sobol', Faure, Niederreiter, Niederreiter and Xing as well as others, see [8, Section 8] for more information. These point sets generally hold good properties of uniform distribution modulo one. The typical convergence rate of the QMC integration error  $|I(f) - Q(f; P)|$  using these point sets is  $O(|P|^{-1+\varepsilon})$  with arbitrarily small  $\varepsilon > 0$ .

Our goal of this paper is to give an explicit means of constructing good deterministic point sets for QMC integration of smooth functions in certain Sobolev spaces  $\mathcal{H}_\alpha$  of smoothness of arbitrarily high order  $\alpha \geq 2$ . For such smooth functions, it is possible to achieve higher order convergence of  $O(|P|^{-\alpha+\varepsilon})$  (with arbitrarily small  $\varepsilon > 0$ ) of the QMC integration error by using *higher order* digital nets [1, 4]. The explicit construction of higher order digital nets introduced in [4] uses digital nets whose number of components is a multiple of the dimension, and interlaces them digitally in a certain way. Another construction of higher order digital nets, known under the name of *higher order polynomial lattice point sets* (HOPLPSs), is introduced in [7] by generalizing the definition of polynomial lattice point sets, which was originally given in [15]. Recently, one of the authors has utilized original polynomial lattice point sets as interlaced components in the former construction principle, and has proved that it is possible to obtain good *interlaced polynomial lattice point sets* (IPLPSs) for higher order digital nets [11], see also [12].

The most important advantage of IPLPSs over HOPLPSs lies in the construction cost. Fast component-by-component (CBC) construction requires  $O(s\alpha|P|\log|P|)$  arithmetic operations using  $O(|P|)$  memory for IPLPSs [11], whereas requiring  $O(s\alpha|P|^\alpha \log|P|)$  arithmetic operations using  $O(|P|^\alpha)$  memory for HOPLPSs [2]. In order to reduce the construction cost for HOPLPSs, one of the authors considered applying a random digital shift and then folding the resulting point sets by using the tent transformation in [10]. (We note that the tent transformation was originally used for lattice rules in [14].) The obtained cost for the fast CBC construction becomes  $O(s\alpha|P|^{\alpha/2} \log|P|)$  arithmetic operations using  $O(|P|^{\alpha/2})$  memory. This is a generalization of the study in [3]. However, this result not only restricts the base  $b$  to 2, but also needs a randomization by a random digital shift. Thus, we cannot construct good *deterministic* point sets in this way in contrast to [2, 11].

Regarding the restriction of the base, the authors have recently introduced the *b-adic tent transformation* (*b*-TT) in [13] for any positive integer  $b \geq 2$ , by generalizing the original (dyadic) tent transformation, and studied the mean square worst-case error of *digitally shifted and then folded* digital nets in reproducing kernel Hilbert spaces. As a continuation of the study in [13], we resolve the above concerns on [10] in this paper.

We first consider QMC point sets which are obtained by folding digital nets by means of the *b*-TT, and study the worst-case error of QMC rules using such

*folded digital nets* in reproducing kernel Hilbert spaces. In our analysis, we need to permit digital nets with “infinite digit expansions”, which are beyond the scope of the classical definition of digital nets, see for example [8, Chapter 4] and [16, Chapter 4]. To overcome this issue, we consider infinite products of cyclic groups  $G$  and the characters on  $G$ , and define digital nets in  $G^s$  by using infinite-column generating matrices, i.e., generating matrices whose each column can contain infinitely many entries different from zero, see Definition 9. Then we discuss the dual net of folded digital nets and the worst-case error in reproducing kernel Hilbert spaces. This is the first contribution of this paper.

Using the results of the above argument, we do the following next. We employ HOPLPSs in prime base  $b$  that are folded using the  $b$ -TT. We call such deterministic point sets *folded higher order polynomial lattice point sets* (FHOPLPSs). We consider the Sobolev space  $\mathcal{H}_\alpha$  as a function space, and prove that the component-by-component construction can find good FHOPLPSs for which QMC integration achieves the optimal convergence rate of the worst-case error in  $\mathcal{H}_\alpha$ . Moreover, we show how to obtain the fast component-by-component construction using the fast Fourier transform in a way analogous to [2, 10]. We obtain a construction cost of the algorithm of  $O(s\alpha|P|^{\alpha/2} \log |P|)$  arithmetic operations using  $O(|P|^{\alpha/2})$  memory. This is the second contribution of this paper. We note that QMC point sets constructed in this way are considered useful in the context of uncertainty quantification, in particular partial differential equations with random coefficients [5], although the investigation of this application is beyond the scope of this paper.

The remainder of this paper is organized as follows. In Section 2, we recall some necessary background and notation, including infinite products of cyclic groups  $G$ , Walsh functions, digital nets, and HOPLPSs. As mentioned above, we define digital nets in  $G^s$ , instead of those in  $[0, 1]^s$ , by using infinite-column generating matrices. In Section 3, we first describe the  $b$ -TT and some properties of folded digital nets, that is, digital nets that are folded by using the  $b$ -TT, and then study the worst-case error of QMC rules using folded digital nets in reproducing kernel Hilbert spaces. In Section 4, we introduce the Sobolev spaces  $\mathcal{H}_\alpha$  and give an upper bound on the worst-case error for QMC rules using folded digital nets in  $\mathcal{H}_\alpha$ . In Section 5, we prove that the CBC construction can find good FHOPLPSs for which QMC integration achieves the optimal convergence rate of the worst-case error in  $\mathcal{H}_\alpha$ . Finally in Section 6, we show how to obtain the fast CBC construction using the fast Fourier transform in a way analogous to [2, 10].

## 2 Preliminaries

Throughout this paper, we use the following notation. Let  $\mathbb{N}$  be the set of positive integers and let  $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ . Let  $\mathbb{C}$  be the set of all complex numbers. For a positive integer  $b \geq 2$ , let  $\mathbb{Z}_b$  be a cyclic group with  $b$  elements, which is identified with the set  $\{0, 1, \dots, b-1\}$  equipped with addition modulo  $b$ .

### 2.1 Infinite products of cyclic groups

This subsection is based on [21], which treats only the one-dimensional dyadic case, and [19], which constructs Pontryagin duality theory for locally compact

abelian groups. First we consider the one-dimensional case. Let us define  $G := \prod_{i=1}^{\infty} \mathbb{Z}_b$ .  $G$  is a compact abelian group with the product topology, where  $\mathbb{Z}_b$  is considered to be a discrete group. We denote by  $\oplus$  and  $\ominus$  addition and subtraction in  $G$ , respectively. Let  $\nu$  be the product measure on  $G$  inherited from the uniform measure on  $\mathbb{Z}_b$ ; For every cylinder set  $E = \prod_{i=1}^n Z_i \times \prod_{i=n+1}^{\infty} \mathbb{Z}_b$  with  $Z_i \subset \mathbb{Z}_b$  ( $1 \leq i \leq n$ ), it holds that  $\nu(E) = \prod_{i=1}^n (|Z_i|/b)$ .

A character on  $G$  is a continuous group homomorphism from  $G$  to  $\{z \in \mathbb{C} : |z| = 1\}$ , which is a multiplicative group of complex numbers whose absolute value is 1. We define the  $k$ -th character  $W_k$  as follows.

**Definition 1.** Let  $b \geq 2$  be a positive integer, and let  $\omega := \exp(2\pi\sqrt{-1}/b)$  be the primitive  $b$ -th root of unity. Let  $z = (\zeta_1, \zeta_2, \dots)^\top \in G$  and  $k \in \mathbb{N}_0$  whose  $b$ -adic expansion is  $k = \kappa_0 + \kappa_1 b + \dots + \kappa_{a-1} b^{a-1}$  with  $\kappa_0, \dots, \kappa_{a-1} \in \mathbb{Z}_b$ . Then the  $k$ -th character  $W_k: G \rightarrow \{1, \omega, \dots, \omega^{b-1}\}$  is given by

$$W_k(z) := \omega^{\kappa_0 \zeta_1 + \dots + \kappa_{a-1} \zeta_a}.$$

We note that every character on  $G$  is equal to some  $W_k$ , see [19].

The group  $G$  can be related to the interval  $[0, 1]$  through two maps  $\pi: G \rightarrow [0, 1]$  and  $\sigma: [0, 1] \rightarrow G$ . Let  $z = (\zeta_1, \zeta_2, \dots)^\top \in G$  and  $x \in [0, 1]$  whose  $b$ -adic expansions are  $x = \sum_{i=1}^{\infty} \xi_i b^{-i}$  with  $\xi_i \in \mathbb{Z}_b$ , which is unique in the sense that infinitely many of the  $\xi_i$  are different from  $b-1$  if  $x \neq 1$  and that all  $\xi_i$  are equal to  $b-1$  if  $x = 1$ . Then the projection map  $\pi: G \rightarrow [0, 1]$  is defined as  $\pi(z) = \sum_{i=1}^{\infty} \zeta_i b^{-i}$  and the section map  $\sigma: [0, 1] \rightarrow G$  is defined as  $\sigma(x) = (\xi_1, \xi_2, \dots)^\top$ . In the dyadic case,  $\sigma$  is called Fine's map. By definition, we have that  $\pi$  is surjective and  $\sigma$  is injective.

These definitions can be generalized to the higher-dimensional case. Let  $G^s$  denote the  $s$ -ary Cartesian product of  $G$ .  $G^s$  is also a compact abelian group with the product topology. The operators  $\oplus$  and  $\ominus$  denote addition and subtraction in  $G^s$ , respectively. We denote by  $\nu$  the product measure on  $G^s$  inherited from  $\nu$ . For integrals on  $G^s$ , we only consider the measure  $\nu$ . Hence, in order to emphasize the variable, we write  $\int_{G^s} f(\mathbf{z}) d\mathbf{z}$  instead of  $\int_{G^s} f d\nu$ . We define the  $\mathbf{k}$ -th character  $W_{\mathbf{k}}$  as follows.

**Definition 2.** Let  $b \geq 2$  be a positive integer. For a dimension  $s \in \mathbb{N}$ , let  $\mathbf{z} = (z_1, \dots, z_s) \in G^s$  and  $\mathbf{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s$ . Then the  $\mathbf{k}$ -th character  $W_{\mathbf{k}}: G^s \rightarrow \{1, \omega_b, \dots, \omega_b^{b-1}\}$  is defined as

$$W_{\mathbf{k}}(\mathbf{z}) := \prod_{j=1}^s W_{k_j}(z_j).$$

Note that every character on  $G^s$  is equal to some  $W_{\mathbf{k}}$  as with the one-dimensional case. For the  $s$ -dimensional projection and section map, we use the same symbol  $\pi$  and  $\sigma$  as in the one-dimensional case. That is, for  $\mathbf{z} = (z_1, \dots, z_s) \in G^s$  and  $\mathbf{x} = (x_1, \dots, x_s) \in [0, 1]^s$ , we define the projection map  $\pi: G^s \rightarrow [0, 1]^s$  as  $\pi(\mathbf{z}) = (\pi(z_1), \dots, \pi(z_s))$  and the section map  $\sigma: [0, 1]^s \rightarrow G^s$  as  $\sigma(\mathbf{x}) = (\sigma(x_1), \dots, \sigma(x_s))$ .

The orthogonality of the characters on  $G^s$  are described below, see [19] for the proof.

**Proposition 3.** The following holds true:

1. For  $k \in \mathbb{N}_0$ , we have

$$\int_G W_k(z) \, dz = \begin{cases} 1 & \text{if } k = 0, \\ 0 & \text{otherwise.} \end{cases}$$

2. For all  $\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s$ , we have

$$\int_{G^s} W_{\mathbf{k}}(z) \overline{W_{\mathbf{l}}(z)} \, dz = \begin{cases} 1 & \text{if } \mathbf{k} = \mathbf{l}, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, we need a lemma on the partial sum of characters referred to as Paley's lemma. Since the proof is essentially the same as [21, Paley's lemma], we omit it.

**Lemma 4.** *Let  $n$  be a positive integer. For  $\mathbf{z} = (z_1, \dots, z_s) \in G^s$  with  $z_i = (\zeta_{i,1}, \zeta_{i,2}, \dots)^\top \in G$ , we have*

$$\sum_{\mathbf{k} < b^n} W_{\mathbf{k}}(\mathbf{z}) = \begin{cases} b^{sn} & \text{if } \zeta_{i,1} = \dots = \zeta_{i,n} = 0 \text{ for all } 1 \leq i \leq s, \\ 0 & \text{otherwise,} \end{cases}$$

where  $\mathbf{k} = (k_1, \dots, k_s) < b^n$  means that  $k_i < b^n$  holds for every  $1 \leq i \leq s$ .

Properties of  $\pi$  and  $\sigma$  are described below.

**Proposition 5.** *We have the following:*

1.  $\pi$  is a continuous map.
2.  $\pi \circ \sigma = \text{id}_{[0,1]^s}$ .
3. For  $f \in L^1(G^s)$ , we have

$$\int_{G^s} f(\mathbf{z}) \, d\mathbf{z} = \int_{[0,1]^s} f(\sigma(\mathbf{x})) \, d\mathbf{x}.$$

4. For  $f \in L^1([0,1]^s)$ , we have

$$\int_{[0,1]^s} f(\mathbf{x}) \, d\mathbf{x} = \int_{G^s} f(\pi(\mathbf{z})) \, d\mathbf{z}.$$

Items 1 and 2 of Proposition 5 follow by definition. For the proof of Items 3 and 4 of Proposition 5, we refer to [21, Theorem 5].

## 2.2 Walsh functions

Walsh functions play a central role in the analysis of digital nets. We refer to [8, Appendix A] for general information on Walsh functions. We first give the definition for the one-dimensional case.

**Definition 6.** Let  $b \geq 2$  be a positive integer and let  $\omega_b = \exp(2\pi\sqrt{-1}/b)$ . We denote the  $b$ -adic expansion of  $k \in \mathbb{N}_0$  by  $k = \kappa_0 + \kappa_1 b + \dots + \kappa_{a-1} b^{a-1}$  with  $\kappa_0, \dots, \kappa_{a-1} \in \mathbb{Z}_b$ . Then the  $k$ -th  $b$ -adic Walsh function  ${}_b\text{wal}_k: [0, 1] \rightarrow \{1, \omega_b, \dots, \omega_b^{b-1}\}$  is defined as

$${}_b\text{wal}_k(x) := \omega_b^{\kappa_0 \xi_1 + \dots + \kappa_{a-1} \xi_a},$$

for  $x \in [0, 1]$  whose  $b$ -adic expansion is given by  $x = \xi_1 b^{-1} + \xi_2 b^{-2} + \dots$ , which is unique in the sense that infinitely many of the  $\xi_i$  are different from  $b-1$  if  $x \neq 1$  and that all  $\xi_i$  are equal to  $b-1$  if  $x = 1$ .

We note that Walsh functions are usually defined on  $[0, 1)$ , whereas they are defined on  $[0, 1]$  specially for this study. This definition can be generalized to the higher-dimensional case.

**Definition 7.** Let  $b \geq 2$  be a positive integer. For a dimension  $s \in \mathbb{N}$ , let  $\mathbf{x} = (x_1, \dots, x_s) \in [0, 1]^s$  and  $\mathbf{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s$ . Then the  $\mathbf{k}$ -th  $b$ -adic Walsh function  ${}_b\text{wal}_{\mathbf{k}}: [0, 1]^s \rightarrow \{1, \omega_b, \dots, \omega_b^{b-1}\}$  is defined as

$${}_b\text{wal}_{\mathbf{k}}(\mathbf{x}) := \prod_{j=1}^s {}_b\text{wal}_{k_j}(x_j).$$

Since we shall always use Walsh functions in a fixed base  $b$ , we omit the subscript and simply write  $\text{wal}_k$  or  $\text{wal}_{\mathbf{k}}$  in this paper. By the definition of characters and Walsh functions, we can see that

$$\text{wal}_{\mathbf{k}}(\mathbf{x}) = W_{\mathbf{k}}(\sigma(\mathbf{x})). \quad (1)$$

Some important properties of Walsh functions, used in this paper, are described below, see [8, Appendix A.2] for the proof.

**Proposition 8.** We have the following:

1. For  $k \in \mathbb{N}_0$ , we have

$$\int_0^1 \text{wal}_k(x) dx = \begin{cases} 1 & \text{if } k = 0, \\ 0 & \text{otherwise.} \end{cases}$$

2. For all  $\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s$ , we have

$$\int_{[0,1]^s} \text{wal}_{\mathbf{k}}(\mathbf{x}) \overline{\text{wal}_{\mathbf{l}}(\mathbf{x})} d\mathbf{x} = \begin{cases} 1 & \text{if } \mathbf{k} = \mathbf{l}, \\ 0 & \text{otherwise.} \end{cases}$$

3. The system  $\{\text{wal}_{\mathbf{k}} : \mathbf{k} \in \mathbb{N}_0^s\}$  is a complete orthonormal system in  $L^2([0, 1]^s)$  for any  $s \in \mathbb{N}$ .

From Item 3 of Proposition 8, we define the Walsh series of  $f \in L^2([0, 1]^s)$  by

$$\sum_{\mathbf{k} \in \mathbb{N}_0^s} \hat{f}(\mathbf{k}) \text{wal}_{\mathbf{k}},$$

where the  $\mathbf{k}$ -th Walsh coefficient is given by

$$\hat{f}(\mathbf{k}) = \int_{[0,1]^s} f(\mathbf{x}) \overline{\text{wal}_{\mathbf{k}}(\mathbf{x})} d\mathbf{x}.$$

We refer to [8, Appendix A.3] and [13, Lemma 17] for a discussion on the pointwise absolute convergence of the Walsh series.

### 2.3 Digital nets

We introduce the general definition of digital nets in  $G^s$  by using infinite-column generating matrices for an arbitrary positive integer  $b \geq 2$ .

**Definition 9.** For  $m \in \mathbb{N}$ , let  $C_1, \dots, C_s \in \mathbb{Z}_b^{\mathbb{N} \times m}$ . For each non-negative integer  $h$  with  $0 \leq h < b^m$ , we denote its  $b$ -adic expansion by  $h = \sum_{i=0}^{m-1} \eta_i b^i$ . Let  $\mathbf{z}_h = (z_{h,1}, \dots, z_{h,s}) \in G^s$  be given by

$$z_{h,j} = C_j \cdot (\eta_0, \eta_1, \dots, \eta_{m-1})^\top,$$

for  $1 \leq j \leq s$ . We call  $\mathcal{P} = \{\mathbf{z}_0, \mathbf{z}_1, \dots, \mathbf{z}_{b^m-1}\}$  a digital net in  $G^s$  with generating matrices  $C_1, \dots, C_s$ .

We note that every digital net in  $G^s$  is a  $\mathbb{Z}_b$ -module of  $G^s$  as well as a subgroup of  $G^s$  by Definition 9. We call  $P \subset [0, 1]^s$  a *digital net in  $[0, 1]^s$  over  $\mathbb{Z}_b$*  if there exists a  $\mathcal{P}$  which is a digital net in  $G^s$  with  $P = \pi(\mathcal{P})$ . In this paper, we use digital nets in  $[0, 1]^s$  over  $\mathbb{Z}_b$  as quadrature points.

**Remark 10.** Historically, (classical) digital nets are subsets of  $[0, 1]^s$  constructed by finite-column generating matrices, i.e., generating matrices whose each column consists of only finitely many entries different from zero. If  $P$  is a classical digital net, we have that  $\sigma(P)$  is a digital net in  $G^s$  and that  $\pi(\sigma(P)) = P$ . Hence a classical digital net  $P$  can be considered as a digital net in  $[0, 1]^s$  over  $\mathbb{Z}_b$ . Our definition of digital nets permits digital nets with “infinite digit expansions”. Although the concept of infinite digit expansions has already appeared in the definition of digital sequences [17, Chapter 8], it has not been discussed for digital nets in the literature as far as the authors know.

The dual net of a digital net plays an important role in the subsequent analysis. For a digital net  $\mathcal{P}$ , its dual net, denoted by  $\mathcal{P}^\perp$ , is defined as follows.

**Definition 11.** Let  $\mathcal{P}$  be a digital net in  $G^s$  with generating matrices  $C_1, \dots, C_s \in \mathbb{Z}_b^{\mathbb{N} \times m}$ . The dual net of  $\mathcal{P}$  is defined as

$$\mathcal{P}^\perp := \{\mathbf{k} \in \mathbb{N}_0^s : C_1^\top \vec{k}_1 \oplus \dots \oplus C_s^\top \vec{k}_s = \mathbf{0} \in \mathbb{Z}_b^m\},$$

where, for  $1 \leq j \leq s$ , we write  $\vec{k}_j = (\kappa_{0,j}, \kappa_{1,j}, \dots)^\top \in G$  for  $k_j$  with its  $b$ -adic expansion  $k_j = \kappa_{0,j} + \kappa_{1,j}b + \dots$ , which is actually a finite expansion.

Using the characters on  $G^s$ , the dual net  $\mathcal{P}^\perp$  is also given by

$$\mathcal{P}^\perp = \{\mathbf{k} \in \mathbb{N}_0^s : W_{\mathbf{k}}(\mathbf{z}) = 1 \text{ for all } \mathbf{z} \in \mathcal{P}\}.$$

A similar definition of the dual net has been introduced in [6, Definition 2.5] for digital nets in  $G^s$  with finite digit expansions. Because of orthogonality of the characters, we have the following.

**Lemma 12.** Let  $\mathcal{P}$  be a digital net in  $G^s$ , and let  $\mathcal{P}^\perp$  be its dual net. Then we have

$$\sum_{\mathbf{z} \in \mathcal{P}} W_{\mathbf{k}}(\mathbf{z}) = \begin{cases} |\mathcal{P}| & \text{if } \mathbf{k} \in \mathcal{P}^\perp, \\ 0 & \text{otherwise.} \end{cases}$$

## 2.4 Higher order polynomial lattice rules

We define higher order polynomial lattice point sets as subsets of  $G^s$ , whose construction is based on rational functions over finite fields [7]. Now let  $b$  be a prime. We denote by  $\mathbb{Z}_b[x]$  the set of all polynomials in  $\mathbb{Z}_b$  and by  $\mathbb{Z}_b((x^{-1}))$  the field of formal Laurent series in  $\mathbb{Z}_b$ . Every element of  $\mathbb{Z}_b((x^{-1}))$  can be expressed in the form

$$L = \sum_{l=w}^{\infty} t_l x^{-l},$$

for some integer  $w$  and  $t_l \in \mathbb{Z}_b$ . When  $w > 1$ , we set  $t_1 = \dots = t_{w-1} = 0$ . For  $n \in \mathbb{N}$ , we define the mapping  $v_n: \mathbb{Z}_b((x^{-1})) \rightarrow G$  by

$$v_n \left( \sum_{l=w}^{\infty} t_l x^{-l} \right) = (t_1, \dots, t_n, 0, 0, \dots)^\top.$$

We shall often identify an integer  $n = n_0 + n_1 b + \dots \in \mathbb{N}_0$  with a polynomial  $n(x) = n_0 + n_1 x + \dots \in \mathbb{Z}_b[x]$ . Then HOPLPSs are constructed as follows.

**Definition 13.** For  $m, n, s \in \mathbb{N}$  with  $m \leq n$  let  $p \in \mathbb{Z}_b[x]$  with  $\deg(p) = n$  and let  $\mathbf{q} = (q_1, \dots, q_s) \in (\mathbb{Z}_b[x])^s$ . A higher order polynomial lattice point set (HOPLPS)  $\mathcal{P}(\mathbf{q}, p) \subset G^s$  is given by

$$\mathbf{z}_h := \left( v_n \left( \frac{h(x)q_1(x)}{p(x)} \right), \dots, v_n \left( \frac{h(x)q_s(x)}{p(x)} \right) \right),$$

for an integer  $0 \leq h < b^m$ , which is identified with  $h(x) \in \mathbb{Z}_b[x]$ . A QMC rule using  $\pi(\mathcal{P}(\mathbf{q}, p))$  is called a higher order polynomial lattice rule with modulus  $p$  and generating vector  $\mathbf{q}$ .

We define the truncated polynomial  $\text{tr}_n(k)$ , associated with  $k \in \mathbb{N}_0$  whose  $b$ -adic expansion is given by  $k = \kappa_0 + \kappa_1 b + \dots$ , as

$$\text{tr}_n(k)(x) = \kappa_0 + \kappa_1 x + \dots + \kappa_{n-1} x^{n-1}.$$

Then the *dual polynomial lattice* of a HOPLPS  $\mathcal{P}(\mathbf{q}, p)$  plays the same role as the dual net of a digital net. It is defined as follows.

**Definition 14.** For  $m, n, s \in \mathbb{N}$  with  $m \leq n$ , let  $\mathcal{P}(\mathbf{q}, p)$  be a HOPLPS. The dual polynomial lattice of  $\mathcal{P}(\mathbf{q}, p)$ , denoted by  $\mathcal{P}^\perp(\mathbf{q}, p)$ , is defined as

$$\mathcal{P}^\perp(\mathbf{q}, p) := \{\mathbf{k} = (k_1, \dots, k_s) \in \mathbb{N}_0^s : \text{tr}_n(k_1)q_1 + \dots + \text{tr}_n(k_s)q_s \equiv a \pmod{p} \text{ with } \deg(a) < n - m\}.$$

Accordingly, Lemma 12 is now replaced by the following lemma.

**Lemma 15.** For  $m, n, s \in \mathbb{N}$  with  $m \leq n$ , let  $\mathcal{P}(\mathbf{q}, p)$  be a HOPLPS, and let  $\mathcal{P}^\perp(\mathbf{q}, p)$  be its dual polynomial lattice. Then we have

$$\sum_{\mathbf{z} \in \mathcal{P}(\mathbf{q}, p)} W_{\mathbf{k}}(\mathbf{z}) = \begin{cases} b^m & \text{if } \mathbf{k} \in \mathcal{P}^\perp(\mathbf{q}, p), \\ 0 & \text{otherwise.} \end{cases}$$



### 3 Folded digital nets and integration error

#### 3.1 The $b$ -adic tent transformation

Let  $b$  be an arbitrary positive integer greater than 1 again. Here we describe the  $b$ -adic tent transformation ( $b$ -TT)  $\Phi_b: G \rightarrow G$ . Previously, the authors introduced the  $b$ -adic tent transformation  $\phi_b: [0, 1] \rightarrow [0, 1]$  in [13]. These two  $b$ -adic tent transformations satisfy  $\pi \circ \Phi_b \circ \sigma = \phi_b$ . Notice that the original (dyadic) tent transformation is given by  $\phi_2(x) = 1 - |2x - 1|$ , see [14].

The  $b$ -TT, which is denoted by  $\Phi_b$ , is defined as follows. Let  $z = (\zeta_1, \zeta_2, \dots)^\top \in G$ . Then  $\Phi_b: G \rightarrow G$  is given by

$$\Phi_b(z) := (\eta_1, \eta_2, \dots)^\top \quad \text{with} \quad \eta_i = \zeta_{i+1} - \zeta_1 \pmod{b}.$$

For a vector  $\mathbf{z} = (z_1, \dots, z_s) \in G^s$ , we define  $\Phi_b(\mathbf{z}) := (\Phi_b(z_1), \dots, \Phi_b(z_s))$ . We can see that  $\Phi_b$  is a  $\mathbb{Z}_b$ -module homomorphism as well as a group homomorphism.

#### 3.2 Folded digital nets

In the following we consider folded digital nets in  $G^s$ , that is, digital nets in  $G^s$  that are folded using the  $b$ -TT. We recall that quadrature points in  $[0, 1]^s$  used for QMC integration are obtained by the mapping  $\pi$ . For the sake of completeness, we give the definition of folded digital nets below.

**Definition 16.** Let  $\mathcal{P}$  be a digital net in  $G^s$ . The folded digital net of  $\mathcal{P}$ , denoted by  $\mathcal{P}_{\Phi_b}$ , is defined as

$$\mathcal{P}_{\Phi_b} := \{\Phi_b(\mathbf{z}) : \mathbf{z} \in \mathcal{P}\}.$$

**Remark 17.** Let  $\mathcal{P}$  be a digital net in  $G^s$  with generating matrices  $C_1, \dots, C_s \in \mathbb{Z}_b^{N \times m}$ . In view of Definition 9, the folded digital net of  $\mathcal{P}$  coincides with the digital net in  $G^s$  with generating matrices  $TC_1, \dots, TC_s \in \mathbb{Z}_b^{N \times m}$ , where the matrix  $T = (t_{i,j})_{i,j \in \mathbb{N}}$  is defined as

$$t_{i,j} = \begin{cases} b-1 & \text{if } j = 1, \\ 1 & \text{if } j = i+1, \\ 0 & \text{otherwise.} \end{cases}$$

This fact has already been utilized to study the  $L_p$  discrepancy of two-dimensional folded Hammersley point sets [9].

We now consider the dual net of folded digital nets. In order to give the following lemma, we need to introduce some notation. For  $x \in \mathbb{R}$ , we denote by  $\lfloor x \rfloor$  the unique integer  $n$  satisfying the inequalities  $n \leq x < n+1$ . For  $\mathbf{x} = (x_1, \dots, x_s) \in \mathbb{R}^s$ , we write  $\lfloor \mathbf{x} \rfloor = (\lfloor x_1 \rfloor, \dots, \lfloor x_s \rfloor)$  for short. For  $k \in \mathbb{N}$  whose  $b$ -adic expansion is given by  $k = \kappa_0 + \kappa_1 b + \dots$ , let  $\delta(k) := \kappa_0 + \kappa_1 + \dots$ , which is called the  $b$ -adic sum-of-digits of  $k$ . Moreover, we define

$$\mathcal{E} := \{k \in \mathbb{N} : \delta(k) \equiv 0 \pmod{b}\},$$

and  $\mathcal{E}_0 := \mathcal{E} \cup \{0\}$ .

**Lemma 18.** *Let  $\mathcal{P}$  be a digital net in  $G^s$ , and let  $\mathcal{P}_{\Phi_b}$  be its folded digital net. Further, let  $\mathcal{P}^\perp$  be the dual net of  $\mathcal{P}$ , and let  $\mathcal{P}_{\Phi_b}^\perp$  be the dual net of  $\mathcal{P}_{\Phi_b}$ . Then we have*

$$\mathcal{P}_{\Phi_b}^\perp = \{ \lfloor \mathbf{k}/b \rfloor : \mathbf{k} \in \mathcal{E}_0^s \cap \mathcal{P}^\perp \},$$

where we write  $\lfloor \mathbf{k}/b \rfloor = (\lfloor k_1/b \rfloor, \dots, \lfloor k_s/b \rfloor)$  for  $\mathbf{k} = (k_1, \dots, k_s)$ .

*Proof.* Let  $\mathcal{P}$  be a digital net in  $G^s$  with generating matrices  $C_1, \dots, C_s$ . From Definition 11 and Remark 17, the dual net  $\mathcal{P}_{\Phi_b}^\perp$  is given by

$$\begin{aligned} \mathcal{P}_{\Phi_b}^\perp &= \{ \mathbf{k} \in \mathbb{N}_0^s : (TC_1)^\top \vec{k}_1 \oplus \dots \oplus (TC_s)^\top \vec{k}_s = \mathbf{0} \in \mathbb{Z}_b^m \} \\ &= \{ \mathbf{k} \in \mathbb{N}_0^s : C_1^\top T^\top \vec{k}_1 \oplus \dots \oplus C_s^\top T^\top \vec{k}_s = \mathbf{0} \in \mathbb{Z}_b^m \}. \end{aligned}$$

For  $1 \leq j \leq s$ , we have

$$T^\top \vec{k}_j = \begin{pmatrix} b-1 & b-1 & b-1 & \cdots \\ 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & \cdots \\ 0 & 0 & 1 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} \begin{pmatrix} \kappa_{0,j} \\ \kappa_{1,j} \\ \kappa_{2,j} \\ \kappa_{3,j} \\ \vdots \end{pmatrix} = \begin{pmatrix} -(\kappa_{0,j} + \kappa_{1,j} + \cdots) \\ \kappa_{0,j} \\ \kappa_{1,j} \\ \kappa_{2,j} \\ \vdots \end{pmatrix}.$$

We now define  $\beta : \mathbb{N}_0 \rightarrow \{0, \dots, b-1\}$  by  $\beta(k) = -\delta(k) \pmod{b}$  for  $k \in \mathbb{N}_0$ . Then we have

$$T^\top \vec{k}_j = \vec{l}_j \in G,$$

where  $l_j$  is given by

$$\begin{aligned} l_j &= \beta(k_j) + \kappa_{0,j}b + \kappa_{1,j}b^2 + \cdots \\ &= \beta(k_j) + bk_j. \end{aligned}$$

Using this notation,  $\mathcal{P}_{\Phi_b}^\perp$  is given by

$$\begin{aligned} \mathcal{P}_{\Phi_b}^\perp &= \{ \mathbf{k} \in \mathbb{N}_0^s : C_1^\top \vec{l}_1 \oplus \dots \oplus C_s^\top \vec{l}_s = \mathbf{0} \in \mathbb{Z}_b^m \} \\ &= \{ \mathbf{k} \in \mathbb{N}_0^s : (l_1, \dots, l_s) \in \mathcal{P}^\perp \}, \end{aligned} \tag{2}$$

where the second equality stems from the definition of the dual net of  $\mathcal{P}$ , see Definition 11. Here we see that

$$\delta(l_j) \equiv -\delta(k_j) + \kappa_0 + \kappa_1 + \cdots \equiv -\delta(k_j) + \delta(k_j) \equiv 0 \pmod{b}.$$

This implies that  $(l_1, \dots, l_s) \in \mathcal{E}_0^s$ . Let us consider the equation  $\delta(k'_j + bk_j) \equiv 0 \pmod{b}$  with a variable  $k'_j \in \{0, \dots, b-1\}$ . It is easy to confirm that  $k'_j = \beta(k_j)$  is the only solution of this equation. Moreover, since we have  $\lfloor (k'_j + bk_j)/b \rfloor = k_j$  independently of the choice  $k'_j \in \{0, \dots, b-1\}$ ,  $k_j$  in (2) can be uniquely expressed as  $\lfloor l_j/b \rfloor$ . Thus we have

$$\mathcal{P}_{\Phi_b}^\perp = \{ \lfloor \mathbf{l}/b \rfloor : \mathbf{l} \in \mathcal{E}_0^s \cap \mathcal{P}^\perp \},$$

which completes the proof.  $\square$

### 3.3 Worst-case error in reproducing kernel Hilbert spaces

Let us consider a reproducing kernel Hilbert space  $\mathcal{H}$  with reproducing kernel  $\mathcal{K} : [0, 1]^s \times [0, 1]^s \rightarrow \mathbb{R}$ . The inner product in  $\mathcal{H}$  is denoted by  $\langle f, g \rangle_{\mathcal{H}}$  for  $f, g \in \mathcal{H}$  and the associated norm is denoted by  $\|f\|_{\mathcal{H}} := \sqrt{\langle f, f \rangle_{\mathcal{H}}}$ .

It is known that if a reproducing kernel  $\mathcal{K}$  satisfies  $\int_{[0,1]^s} \sqrt{\mathcal{K}(\mathbf{x}, \mathbf{x})} d\mathbf{x} < \infty$  the squared worst-case error in the space  $\mathcal{H}$  of the QMC rule using a point set  $P \subset [0, 1]^s$  is given by

$$\begin{aligned} e^2(P, \mathcal{K}) &:= \left( \sup_{\substack{f \in \mathcal{H} \\ \|f\|_{\mathcal{H}} \leq 1}} |I(f) - Q(f; P)| \right)^2 \\ &= \int_{[0,1]^{2s}} \mathcal{K}(\mathbf{x}, \mathbf{y}) d\mathbf{x} d\mathbf{y} - \frac{2}{|P|} \sum_{\mathbf{x} \in P} \int_{[0,1]^s} \mathcal{K}(\mathbf{x}, \mathbf{y}) d\mathbf{y} + \frac{1}{|P|^2} \sum_{\mathbf{x}, \mathbf{y} \in P} \mathcal{K}(\mathbf{x}, \mathbf{y}), \quad (3) \end{aligned}$$

while the squared initial error is given by

$$e^2(\emptyset, \mathcal{K}) := \left( \sup_{\substack{f \in \mathcal{H} \\ \|f\|_{\mathcal{H}} \leq 1}} |I(f)| \right)^2 = \int_{[0,1]^{2s}} \mathcal{K}(\mathbf{x}, \mathbf{y}) d\mathbf{x} d\mathbf{y}.$$

For  $\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s$ , the  $(\mathbf{k}, \mathbf{l})$ -th Walsh coefficient of  $\mathcal{K}$  is given by

$$\hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) := \int_{[0,1]^{2s}} \mathcal{K}(\mathbf{x}, \mathbf{y}) \overline{\text{wal}_{\mathbf{k}}(\mathbf{x})} \text{wal}_{\mathbf{l}}(\mathbf{y}) d\mathbf{x} d\mathbf{y}.$$

We refer to [8, Chapter 2] for details. In the following we always assume  $\int_{[0,1]^s} \sqrt{\mathcal{K}(\mathbf{x}, \mathbf{x})} d\mathbf{x} < \infty$  and consider the squared worst-case error of QMC rules using digital nets in  $[0, 1]^s$  in the space  $\mathcal{H}$ .

**Proposition 19.** *Let  $\mathcal{P}, \mathcal{P}^\perp$  be a digital net in  $G^s$  and its dual net, respectively, and let  $\mathcal{K}$  be a continuous reproducing kernel which satisfies  $\int_{[0,1]^s} \sqrt{\mathcal{K}(\mathbf{x}, \mathbf{x})} d\mathbf{x} < \infty$ . We assume that  $\sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} |\hat{\mathcal{K}}(\mathbf{k}, \mathbf{l})| < \infty$ . Then the squared worst-case error of QMC rules using  $\pi(\mathcal{P})$  is given by*

$$e^2(\pi(\mathcal{P}), \mathcal{K}) = \sum_{\mathbf{k}, \mathbf{l} \in \mathcal{P}^\perp \setminus \{\mathbf{0}\}} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}).$$

*Proof.* First we prove that for any  $\mathbf{z}, \mathbf{w} \in G^s$  it holds that

$$\mathcal{K}(\pi(\mathbf{z}), \pi(\mathbf{w})) = \sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})}. \quad (4)$$

The proof of (4) is similar to [8, Proposition A.20]. By the assumption that  $\sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} |\hat{\mathcal{K}}(\mathbf{k}, \mathbf{l})| < \infty$ ,  $\sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})}$  converges absolutely. Therefore it suffices to show that

$$\lim_{n \rightarrow \infty} \sum_{\mathbf{k}, \mathbf{l} < b^n} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})} = \mathcal{K}(\pi(\mathbf{z}), \pi(\mathbf{w})),$$

where  $\mathbf{k} = (k_1, \dots, k_s) < b^n$  means that  $k_j < b^n$  holds for every  $j$ . Define two sets  $H_n \subset G$  and  $H(\mathbf{z}, \mathbf{w}, n) \subset G^{2s}$  as  $H_n := \{(\zeta'_1, \zeta'_2, \dots)^\top \in G: \zeta'_1 = \dots = \zeta'_n = 0\}$  and  $H(\mathbf{z}, \mathbf{w}, n) := \{(\mathbf{z}', \mathbf{w}') \in G^{2s}: \mathbf{z} \ominus \mathbf{z}' \in H_n^s, \mathbf{w} \ominus \mathbf{w}' \in H_n^s\}$ . Then we have

$$\begin{aligned}
& \sum_{\mathbf{k}, \mathbf{l} < b^n} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})} \\
&= \sum_{\mathbf{k}, \mathbf{l} < b^n} W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})} \int_{[0,1]^{2s}} \mathcal{K}(\mathbf{x}, \mathbf{y}) \overline{\text{wal}_{\mathbf{k}}(\mathbf{x})} \text{wal}_{\mathbf{l}}(\mathbf{y}) \, d\mathbf{x} \, d\mathbf{y} \\
&= \sum_{\mathbf{k}, \mathbf{l} < b^n} W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})} \int_{[0,1]^{2s}} (\mathcal{K} \circ \pi \circ \sigma)(\mathbf{x}, \mathbf{y}) \overline{W_{\mathbf{k}}(\sigma(\mathbf{x}))} W_{\mathbf{l}}(\sigma(\mathbf{y})) \, d\mathbf{x} \, d\mathbf{y} \\
&= \sum_{\mathbf{k}, \mathbf{l} < b^n} W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})} \int_{G^{2s}} (\mathcal{K} \circ \pi)(\mathbf{z}', \mathbf{w}') \overline{W_{\mathbf{k}}(\mathbf{z}')} W_{\mathbf{l}}(\mathbf{w}') \, d\mathbf{z}' \, d\mathbf{w}' \\
&= \int_{G^{2s}} \mathcal{K}(\pi(\mathbf{z}'), \pi(\mathbf{w}')) \sum_{\mathbf{k}, \mathbf{l} < b^n} \overline{W_{\mathbf{k}}(\mathbf{z}')} W_{\mathbf{l}}(\mathbf{w}') W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})} \, d\mathbf{z}' \, d\mathbf{w}' \\
&= \int_{G^{2s}} \mathcal{K}(\pi(\mathbf{z}'), \pi(\mathbf{w}')) \sum_{\mathbf{k} < b^n} W_{\mathbf{k}}(\mathbf{z} \ominus \mathbf{z}') \sum_{\mathbf{l} < b^n} \overline{W_{\mathbf{l}}(\mathbf{w} \ominus \mathbf{w}')} \, d\mathbf{z}' \, d\mathbf{w}' \\
&= b^{2sn} \int_{H(\mathbf{z}, \mathbf{w}, n)} \mathcal{K}(\pi(\mathbf{z}'), \pi(\mathbf{w}')) \, d\mathbf{z}' \, d\mathbf{w}',
\end{aligned}$$

where we use Item 2 of Proposition 5 and (1), Item 3 of Proposition 5 and Lemma 4 in the second, third and the last equality, respectively. Since  $\mathcal{K}$  and  $\pi$  are continuous,  $\mathcal{K} \circ \pi$  is also continuous. Hence the last term of the above equality converges to  $\mathcal{K}(\pi(\mathbf{z}), \pi(\mathbf{w}))$  as  $n \rightarrow \infty$ . This proves (4).

Now we prove Proposition 19. For the first term on the right-hand side of (3), we have

$$\int_{[0,1]^{2s}} \mathcal{K}(\mathbf{x}, \mathbf{y}) \, d\mathbf{x} \, d\mathbf{y} = \hat{\mathcal{K}}(\mathbf{0}, \mathbf{0}).$$

For the second term on the right-hand side of (3), we have

$$\begin{aligned}
& \frac{2}{|\mathcal{P}|} \sum_{\mathbf{x} \in \pi(\mathcal{P})} \int_{[0,1]^s} \mathcal{K}(\mathbf{x}, \mathbf{y}) \, d\mathbf{y} \\
&= \frac{1}{|\mathcal{P}|} \sum_{\mathbf{x} \in \pi(\mathcal{P})} \int_{[0,1]^s} \mathcal{K}(\mathbf{x}, \mathbf{y}) \, d\mathbf{y} + \frac{1}{|\mathcal{P}|} \sum_{\mathbf{x} \in \pi(\mathcal{P})} \int_{[0,1]^s} \mathcal{K}(\mathbf{y}, \mathbf{x}) \, d\mathbf{y} \\
&= \frac{1}{|\mathcal{P}|} \sum_{\mathbf{z} \in \mathcal{P}} \int_{G^s} \mathcal{K}(\pi(\mathbf{z}), \pi(\mathbf{w})) \, d\mathbf{w} + \frac{1}{|\mathcal{P}|} \sum_{\mathbf{z} \in \mathcal{P}} \int_{G^s} \mathcal{K}(\pi(\mathbf{w}), \pi(\mathbf{z})) \, d\mathbf{w} \\
&= \frac{1}{|\mathcal{P}|} \sum_{\mathbf{z} \in \mathcal{P}} \sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) W_{\mathbf{k}}(\mathbf{z}) \int_{G^s} \overline{W_{\mathbf{l}}(\mathbf{w})} \, d\mathbf{w} \\
&\quad + \frac{1}{|\mathcal{P}|} \sum_{\mathbf{z} \in \mathcal{P}} \sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) \overline{W_{\mathbf{l}}(\mathbf{z})} \int_{G^s} W_{\mathbf{k}}(\mathbf{w}) \, d\mathbf{w} \\
&= \sum_{\mathbf{k} \in \mathbb{N}_0^s} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{0}) \frac{1}{|\mathcal{P}|} \sum_{\mathbf{z} \in \mathcal{P}} W_{\mathbf{k}}(\mathbf{z}) + \sum_{\mathbf{l} \in \mathbb{N}_0^s} \hat{\mathcal{K}}(\mathbf{0}, \mathbf{l}) \frac{1}{|\mathcal{P}|} \sum_{\mathbf{z} \in \mathcal{P}} \overline{W_{\mathbf{l}}(\mathbf{z})}
\end{aligned}$$

$$= \sum_{\mathbf{k} \in \mathcal{P}^\perp} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{0}) + \sum_{\mathbf{l} \in \mathcal{P}^\perp} \hat{\mathcal{K}}(\mathbf{0}, \mathbf{l}),$$

where we use the symmetry of  $\mathcal{K}$ , Item 4 of Proposition 5, (4), Item 1 of Proposition 3 and Lemma 12 in the first, second, third, fourth and fifth equalities, respectively. For the last term on the right-hand side of (3), we have

$$\begin{aligned} \frac{1}{|\mathcal{P}|^2} \sum_{\mathbf{x}, \mathbf{y} \in \pi(\mathcal{P})} \mathcal{K}(\mathbf{x}, \mathbf{y}) &= \frac{1}{|\mathcal{P}|^2} \sum_{\mathbf{z}, \mathbf{w} \in \mathcal{P}} \mathcal{K}(\pi(\mathbf{z}), \pi(\mathbf{w})) \\ &= \frac{1}{|\mathcal{P}|^2} \sum_{\mathbf{z}, \mathbf{w} \in \mathcal{P}} \sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) W_{\mathbf{k}}(\mathbf{z}) \overline{W_{\mathbf{l}}(\mathbf{w})} \\ &= \sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}) \frac{1}{|\mathcal{P}|} \sum_{\mathbf{z} \in \mathcal{P}} W_{\mathbf{k}}(\mathbf{z}) \overline{\frac{1}{|\mathcal{P}|} \sum_{\mathbf{w} \in \mathcal{P}} W_{\mathbf{l}}(\mathbf{w})} \\ &= \sum_{\mathbf{k}, \mathbf{l} \in \mathcal{P}^\perp} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}), \end{aligned}$$

where we use (4) and Lemma 12 again in the second and forth equality, respectively. Substituting these results into the right-hand side of (3), the result follows.  $\square$

As mentioned in Remark 17, when  $\mathcal{P}$  is a digital net in  $G^s$ , its folded digital net  $\mathcal{P}_{\Phi_b}$  is also a digital net in  $G^s$ . Therefore, Proposition 19 can be applied to QMC rules using folded digital nets. We have the following results.

**Proposition 20.** *Let  $\mathcal{P}, \mathcal{P}_{\Phi_b}$  be a digital net in  $G^s$  and its folded digital net, respectively, and let  $\mathcal{P}^\perp$  be the dual net of  $\mathcal{P}$ . Further, let  $\mathcal{K}$  be a continuous reproducing kernel which satisfies  $\int_{[0,1]^s} \sqrt{\mathcal{K}(\mathbf{x}, \mathbf{x})} d\mathbf{x} < \infty$ . Assume that  $\sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} |\hat{\mathcal{K}}(\mathbf{k}, \mathbf{l})| < \infty$ . Then the squared worst-case error of QMC rules using  $\pi(\mathcal{P}_{\Phi_b})$  is given by*

$$e^2(\pi(\mathcal{P}_{\Phi_b}), \mathcal{K}) = \sum_{\mathbf{k}, \mathbf{l} \in \mathcal{E}_0^s \cap \mathcal{P}^\perp \setminus \{\mathbf{0}\}} \hat{\mathcal{K}}(\lfloor \mathbf{k}/b \rfloor, \lfloor \mathbf{l}/b \rfloor).$$

*Proof.* Since  $\mathcal{P}_{\Phi_b}$  is a digital net in  $G^s$ , we have from Proposition 19

$$e^2(\pi(\mathcal{P}_{\Phi_b}), \mathcal{K}) = \sum_{\mathbf{k}, \mathbf{l} \in \mathcal{P}_{\Phi_b}^\perp \setminus \{\mathbf{0}\}} \hat{\mathcal{K}}(\mathbf{k}, \mathbf{l}),$$

where  $\mathcal{P}_{\Phi_b}^\perp$  is the dual net of  $\mathcal{P}_{\Phi_b}$ . Applying Lemma 18 to the right-hand side, we have the result.  $\square$

## 4 Bound on the worst-case error in $\mathcal{H}_\alpha$

### 4.1 Unanchored Sobolev spaces $\mathcal{H}_\alpha$

First we follow the expositions of [1, 7] to introduce the reproducing kernel Hilbert space  $\mathcal{H}_\alpha$  that we consider in the remainder of this paper.

Let  $\alpha$  be a positive integer greater than 1. For the one-dimensional unweighted case, the inner product of  $\mathcal{H}_\alpha$  is given by

$$\langle f, g \rangle_{\mathcal{H}_\alpha} = \sum_{\tau=0}^{\alpha-1} \int_0^1 f^{(\tau)}(x) dx \int_0^1 g^{(\tau)}(x) dx + \int_0^1 f^{(\alpha)}(x) g^{(\alpha)}(x) dx,$$

where  $f^{(\tau)}$  denotes the  $\tau$ -th derivative of  $f$  and  $f^{(0)} = f$ . The reproducing kernel is  $1 + \mathcal{K}_{\alpha,(1)}(\cdot, \cdot)$  for the function  $\mathcal{K}_{\alpha,(1)} : [0, 1] \times [0, 1] \rightarrow \mathbb{R}$  defined as

$$\mathcal{K}_{\alpha,(1)}(x, y) := \sum_{\tau=1}^{\alpha} \frac{\mathcal{B}_\tau(x) \mathcal{B}_\tau(y)}{(\tau!)^2} + (-1)^{\alpha+1} \frac{\mathcal{B}_{2\alpha}(|x-y|)}{(2\alpha)!},$$

for  $x, y \in [0, 1]$ , where  $\mathcal{B}_\tau$  denotes the Bernoulli polynomial of degree  $\tau$ .

Let us consider the  $s$ -dimensional weighted case. Let  $\gamma_1, \dots, \gamma_s$  be non-negative real numbers called *weights*, which moderate the relative importance of different variables in the space  $\mathcal{H}_\alpha$ . For a vector  $(\alpha_1, \dots, \alpha_s) \in \mathbb{N}_0^s$  with  $0 \leq \alpha_j \leq \alpha$  for  $1 \leq j \leq s$ , we denote by  $f^{(\alpha_1, \dots, \alpha_s)}$  the partial mixed derivative of  $f$  of  $(\alpha_1, \dots, \alpha_s)$ -th order. Now the inner product of  $\mathcal{H}_\alpha$  is given by

$$\begin{aligned} \langle f, g \rangle_{\mathcal{H}_\alpha} = & \sum_{u \subseteq \{1, \dots, s\}} \left( \prod_{j \in u} \gamma_j^{-1} \right) \sum_{v \subseteq u} \sum_{\tau_{u \setminus v} \in \{1, \dots, \alpha-1\}^{|u \setminus v|}} \\ & \int_{[0,1]^{|v|}} \left( \int_{[0,1]^{s-|v|}} f^{(\tau_{u \setminus v}, \alpha_v, \mathbf{0})}(\mathbf{x}) d\mathbf{x}_{-v} \right) \\ & \times \left( \int_{[0,1]^{s-|v|}} g^{(\tau_{u \setminus v}, \alpha_v, \mathbf{0})}(\mathbf{x}) d\mathbf{x}_{-v} \right) d\mathbf{x}_v, \end{aligned}$$

where we use the following notation: For  $\tau_{u \setminus v} = (\tau_j)_{j \in u \setminus v}$ , we denote by  $(\tau_{u \setminus v}, \alpha_v, \mathbf{0})$  the vector in which the  $j$ -th component is  $\tau_j$  for  $j \in u \setminus v$ ,  $\alpha$  for  $j \in v$ , and 0 for  $\{1, \dots, s\} \setminus u$ . For  $v \subseteq \{1, \dots, s\}$ , we simply write  $-v := \{1, \dots, s\} \setminus v$ ,  $\mathbf{x}_v = (x_j)_{j \in v}$  and  $\mathbf{x}_{-v} = (x_j)_{j \in -v}$ . Further for  $u \subseteq \{1, \dots, s\}$  such that  $\gamma_j = 0$  for some  $j \in u$ , we assume that the corresponding inner double sum equals 0 and we set  $0/0 = 0$ . The reproducing kernel is given by

$$\mathcal{K}_\alpha(\mathbf{x}, \mathbf{y}) = \prod_{j=1}^s (1 + \gamma_j \mathcal{K}_{\alpha,(1)}(x_j, y_j)),$$

for  $\mathbf{x} = (x_1, \dots, x_s), \mathbf{y} = (y_1, \dots, y_s) \in [0, 1]^s$ . Here we call  $\mathcal{H}_\alpha$  a weighted unanchored Sobolev space of smoothness of order  $\alpha$ .

We now consider a Walsh series expansion of  $\mathcal{K}_\alpha$ ,

$$\begin{aligned} & \sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} \hat{\mathcal{K}}_\alpha(\mathbf{k}, \mathbf{l}) \text{wal}_{\mathbf{k}}(\mathbf{x}) \overline{\text{wal}_{\mathbf{l}}(\mathbf{y})} \\ = & \sum_{u, v \subseteq \{1, \dots, s\}} \sum_{\mathbf{k}_u \in \mathbb{N}^{|u|}} \sum_{\mathbf{l}_v \in \mathbb{N}^{|v|}} \hat{\mathcal{K}}_\alpha((\mathbf{k}_u, \mathbf{0}), (\mathbf{l}_v, \mathbf{0})) \text{wal}_{(\mathbf{k}_u, \mathbf{0})}(\mathbf{x}) \overline{\text{wal}_{(\mathbf{l}_v, \mathbf{0})}(\mathbf{y})}, \end{aligned}$$

where we denote by  $(\mathbf{k}_u, \mathbf{0})$  the  $s$ -dimensional vector whose  $j$ -th component is  $k_j$  if  $j \in u$  and zero otherwise, and we use the same notation for  $(\mathbf{l}_v, \mathbf{0})$ .

According to [1, Lemma 14], for  $u, v \subseteq \{1, \dots, s\}$ ,  $\mathbf{k}_u \in \mathbb{N}^{|u|}$  and  $\mathbf{l}_v \in \mathbb{N}^{|v|}$ , the  $((\mathbf{k}_u, \mathbf{0}), (\mathbf{l}_v, \mathbf{0}))$ -th Walsh coefficient is given by

$$\hat{\mathcal{K}}_\alpha((\mathbf{k}_u, \mathbf{0}), (\mathbf{l}_v, \mathbf{0})) = \begin{cases} \gamma_u \prod_{j \in u} \hat{\mathcal{K}}_{\alpha, (1)}(k_j, l_j) & \text{if } u = v, \\ 0 & \text{otherwise.} \end{cases} \quad (5)$$

Here we write  $\gamma_u = \prod_{j \in u} \gamma_j$  for  $u \subseteq \{1, \dots, s\}$ , where the empty product equals 1. A bound on the Walsh coefficients  $\hat{\mathcal{K}}_{\alpha, (1)}(k, l)$  for  $k, l \in \mathbb{N}$  is given in [1, Section 3] by

$$\left| \hat{\mathcal{K}}_{\alpha, (1)}(k, l) \right| \leq D_{\alpha, b} b^{-\mu_\alpha(k) - \mu_\alpha(l)}, \quad (6)$$

where  $D_{\alpha, b}$  is positive and depends only on  $\alpha$  and  $b$ , which can be calculated explicitly, and  $\mu_\alpha(k)$  is defined for  $k \in \mathbb{N}$  as

$$\mu_\alpha(k) = a_1 + \dots + a_{\min(v, \alpha)},$$

where we denote the  $b$ -adic expansion of  $k$  by  $k = \kappa_1 b^{a_1-1} + \dots + \kappa_v b^{a_v-1}$  with  $0 < \kappa_1, \dots, \kappa_v < b$  and  $a_1 > \dots > a_v > 0$ .

Here  $\mathcal{K}_\alpha$  is continuous in the usual topology of  $[0, 1]^s$ . Therefore, we have  $\int_{[0, 1]^s} \sqrt{\mathcal{K}_\alpha(\mathbf{x}, \mathbf{x})} d\mathbf{x} < \infty$ , and  $\sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} |\hat{\mathcal{K}}_\alpha(\mathbf{k}, \mathbf{l})|$  is also finite since

$$\begin{aligned} \sum_{\mathbf{k}, \mathbf{l} \in \mathbb{N}_0^s} |\hat{\mathcal{K}}_\alpha(\mathbf{k}, \mathbf{l})| &\leq \sum_{u \subseteq \{1, \dots, s\}} \gamma_u D_{\alpha, b}^{|u|} \sum_{\mathbf{k}_u, \mathbf{l}_u \in \mathbb{N}^{|u|}} \prod_{j \in u} b^{-\mu_\alpha(k_j) - \mu_\alpha(l_j)} \\ &= \sum_{u \subseteq \{1, \dots, s\}} \prod_{j \in u} \gamma_j D_{\alpha, b} \left( \sum_{k=1}^{\infty} b^{-\mu_\alpha(k)} \right)^2 \\ &= \prod_{j=1}^s \left[ 1 + \gamma_j D_{\alpha, b} \left( \sum_{k=1}^{\infty} b^{-\mu_\alpha(k)} \right)^2 \right], \end{aligned}$$

where the inner sum is shown to be finite as in [7, Lemma 4.2]. Thus we can apply Proposition 20 to the reproducing kernel  $\mathcal{K}_\alpha$ .

## 4.2 Bound on the worst-case error

Now we show that the worst-case error in  $\mathcal{H}_\alpha$  of QMC rules using  $\pi(\mathcal{P}_{\Phi_b})$  is bounded from above as follows.

**Theorem 21.** *Let  $\mathcal{P}, \mathcal{P}_{\Phi_b}$  be a digital net in  $G^s$  and its folded digital net, respectively, and let  $\mathcal{P}^\perp$  be the dual net of  $\mathcal{P}$ . Then the worst-case error of QMC rules using  $\pi(\mathcal{P}_{\Phi_b})$  in  $\mathcal{H}_\alpha$  is bounded by*

$$e(\pi(\mathcal{P}_{\Phi_b}), \mathcal{K}_\alpha) \leq \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u^{1/2} D_{\alpha, b}^{|u|/2} \sum_{\substack{\mathbf{k}_u \in \mathcal{E}^{|u|} \\ (\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}^\perp}} b^{-\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor)},$$

where we write  $\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor) = \sum_{j \in u} \mu_\alpha(\lfloor k_j/b \rfloor)$ .

*Proof.* Since  $\mathcal{K}_\alpha$  satisfies all the assumptions in Proposition 20, we can use the result of Proposition 20, (5) and (6), in this order, to obtain

$$\begin{aligned}
e^2(\pi(\mathcal{P}_{\Phi_b}), \mathcal{K}_\alpha) &= \sum_{\mathbf{k}, \mathbf{l} \in \mathcal{E}_0^s \cap \mathcal{P}^\perp \setminus \{\mathbf{0}\}} \hat{\mathcal{K}}(\lfloor \mathbf{k}/b \rfloor, \lfloor \mathbf{l}/b \rfloor) \\
&= \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \sum_{\substack{\mathbf{k}_u, \mathbf{l}_u \in \mathcal{E}^{[u]} \\ (\mathbf{k}_u, \mathbf{0}), (\mathbf{l}_u, \mathbf{0}) \in \mathcal{P}^\perp}} \hat{\mathcal{K}}(\lfloor \mathbf{k}_u/b \rfloor, \mathbf{0}), (\lfloor \mathbf{l}_u/b \rfloor, \mathbf{0})) \\
&\leq \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u D_{\alpha, b}^{[u]} \sum_{\substack{\mathbf{k}_u, \mathbf{l}_u \in \mathcal{E}^{[u]} \\ (\mathbf{k}_u, \mathbf{0}), (\mathbf{l}_u, \mathbf{0}) \in \mathcal{P}^\perp}} b^{-\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor) - \mu_\alpha(\lfloor \mathbf{l}_u/b \rfloor)} \\
&= \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u D_{\alpha, b}^{[u]} \left( \sum_{\substack{\mathbf{k}_u \in \mathcal{E}^{[u]} \\ (\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}^\perp}} b^{-\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor)} \right)^2 \\
&\leq \left( \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u^{1/2} D_{\alpha, b}^{[u]/2} \sum_{\substack{\mathbf{k}_u \in \mathcal{E}^{[u]} \\ (\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}^\perp}} b^{-\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor)} \right)^2.
\end{aligned}$$

Thus the result follows.  $\square$

## 5 Component-by-component construction

In this section, we investigate the component-by-component (CBC) construction as an explicit means of constructing good FHOPLPs. More precisely, we attempt to find good HOPLPs  $\mathcal{P}(\mathbf{q}, p)$  by using the CBC construction algorithm, such that QMC rules using those folded point sets (FHOPLPs) in  $[0, 1]^s$ , denoted by  $\pi(\mathcal{P}_{\Phi_b}(\mathbf{q}, p))$ , achieve a good convergence rate of the worst-case error in  $\mathcal{H}_\alpha$ . As above, we write

$$\mathcal{P}_{\Phi_b}(\mathbf{q}, p) := \{\Phi_b(\mathbf{z}) : \mathbf{z} \in \mathcal{P}(\mathbf{q}, p)\}.$$

For this purpose, we employ the bound of the worst-case error shown in Theorem 21 as a quality criterion of  $\mathcal{P}(\mathbf{q}, p)$ . In order to emphasize the role of a modulus  $p \in \mathbb{Z}_b[x]$  and a generating vector  $\mathbf{q} \in (\mathbb{Z}_b[x])^s$  of HOPLPs, we simply write the bound on  $e^2(\pi(\mathcal{P}_{\Phi_b}(\mathbf{q}, p)), \mathcal{K}_\alpha)$  as

$$B_\alpha(\mathbf{q}, p) = \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u^{1/2} D_{\alpha, b}^{[u]/2} \sum_{\substack{\mathbf{k}_u \in \mathcal{E}^{[u]} \\ (\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}^\perp(\mathbf{q}, p)}} b^{-\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor)}.$$

In the following let  $b$  be a prime. We write  $\mathbf{q}_\tau = (q_1, \dots, q_\tau) \in (\mathbb{Z}_b[x])^\tau$  for  $\tau \in \mathbb{N}_0$ , where  $\mathbf{q}_0$  denotes the empty set, and define

$$B_\alpha(\mathbf{q}_\tau, p) := \sum_{\emptyset \neq u \subseteq \{1, \dots, \tau\}} \gamma_u^{1/2} D_{\alpha, b}^{[u]/2} \sum_{\substack{\mathbf{k}_u \in \mathcal{E}^{[u]} \\ (\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}^\perp(\mathbf{q}_\tau, p)}} b^{-\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor)},$$



for  $1 \leq \tau \leq s$ , where we denote by  $(\mathbf{k}_u, \mathbf{0})$  the  $\tau$ -dimensional vector in which the  $j$ -th component is  $k_j$  for  $j \in u$  and 0 for  $j \in \{1, \dots, \tau\} \setminus u$ . In view of Definition 13, we can restrict ourselves to considering each  $q_j \in \mathbb{Z}_b[x]$  such that  $\deg(q_j) < n$  without loss of generality. We write

$$R_{b,n} := \{q \in \mathbb{Z}_b[x] : \deg(q) < n\}.$$

Then the CBC construction proceeds as follows.

**Algorithm 22.** *Let  $b$  be a prime. For  $s, m, n, \alpha \in \mathbb{N}$  with  $\alpha \geq 2$  and  $n \geq m$ , do the following:*

1. *Choose an irreducible polynomial  $p \in \mathbb{Z}_b[x]$  such that  $\deg(p) = n$ .*
2. *For  $\tau = 1, \dots, s$ , assume that  $\mathbf{q}_{\tau-1}$  have already been found. Choose  $q_\tau \in R_{b,n}$  which minimizes  $B_\alpha((\mathbf{q}_{\tau-1}, \tilde{q}_\tau), p)$  as a function of  $\tilde{q}_\tau$ .*

The following theorem gives an upper bound on the worst-case error in  $\mathcal{H}_\alpha$  of FHOPLPS for  $\mathbf{q}$  and  $p$  that are found according to Algorithm 22.

**Theorem 23.** *Let  $b$  be a prime. For  $1 \leq \tau \leq s$ , let  $p \in \mathbb{Z}_b[x]$  and  $\mathbf{q}_\tau \in R_{b,n}^\tau$  be found according to Algorithm 22. Then we have*

$$B_\alpha(\mathbf{q}_\tau, p) \leq \frac{1}{b^{\min(m/\lambda, 2n)}} \left[ -1 + \prod_{j=1}^{\tau} \left( 1 + \gamma_j^{\lambda/2} D_{\alpha,b}^{\lambda/2} A_{\alpha,b,\lambda} \right) \right]^{1/\lambda},$$

for any  $1/\alpha < \lambda \leq 1$ , where  $A_{\alpha,b,\lambda}$  is positive and depends only on  $\alpha, b$  and  $\lambda$ .

The proof of this theorem is given in Appendix A.

**Remark 24.** *Let  $p \in \mathbb{Z}_b[x]$  and  $\mathbf{q} \in R_{b,n}^s$  be found according to Algorithm 22. When  $n \geq \alpha m/2$ , we have  $\min(m/\lambda, 2n) = m/\lambda$  so that*

$$B_\alpha(\mathbf{q}, p) \leq \frac{1}{b^{m/\lambda}} \left[ -1 + \prod_{j=1}^s \left( 1 + \gamma_j^{\lambda/2} D_{\alpha,b}^{\lambda/2} A_{\alpha,b,\lambda} \right) \right]^{1/\lambda},$$

for  $1/\alpha < \lambda \leq 1$ . Since we cannot achieve the convergence rate of the worst-case error of order  $b^{-\alpha m}$  in  $\mathcal{H}_\alpha$  [20], our result is optimal. The degree of the modulus required to achieve the optimal rate of the worst-case error is reduced by half as compared to that obtained in [2, Theorem 1].

## 6 Fast construction algorithm

Finally, in this section, we discuss how to calculate  $B_\alpha(\mathbf{q}, p)$  efficiently and how to obtain the fast CBC construction using the fast Fourier transform.

### 6.1 Efficient calculation of the quality criterion

From Lemma 18 and the definition of  $B_\alpha(\mathbf{q}, p)$ , we have

$$B_\alpha(\mathbf{q}, p) = \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u^{1/2} D_{\alpha,b}^{|u|/2} \sum_{\substack{\mathbf{k}_u \in \mathbb{N}^{|u|} \\ (\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}_{\Phi_b}^\perp(\mathbf{q}, p)}} b^{-\mu_\alpha(\mathbf{k}_u)},$$

where  $\mathcal{P}_{\Phi_b}^\perp(\mathbf{q}, p)$  is the dual net of  $\mathcal{P}_{\Phi_b}(\mathbf{q}, p)$ . Using Lemma 12, we have

$$\begin{aligned}
B_\alpha(\mathbf{q}, p) &= \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u^{1/2} D_{\alpha, b}^{|u|/2} \sum_{\mathbf{k}_u \in \mathbb{N}^{|u|}} b^{-\mu_\alpha(\mathbf{k}_u)} \frac{1}{b^m} \sum_{\mathbf{z} \in \mathcal{P}_{\Phi_b}(\mathbf{q}, p)} W_{(\mathbf{k}_u, \mathbf{0})}(\mathbf{z}) \\
&= \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u^{1/2} D_{\alpha, b}^{|u|/2} \sum_{\mathbf{k}_u \in \mathbb{N}^{|u|}} b^{-\mu_\alpha(\mathbf{k}_u)} \frac{1}{b^m} \sum_{\mathbf{z} \in \mathcal{P}(\mathbf{q}, p)} W_{(\mathbf{k}_u, \mathbf{0})}(\Phi_b(\mathbf{z})) \\
&= \frac{1}{b^m} \sum_{\mathbf{z} \in \mathcal{P}(\mathbf{q}, p)} \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \gamma_u^{1/2} D_{\alpha, b}^{|u|/2} \sum_{\mathbf{k}_u \in \mathbb{N}^{|u|}} b^{-\mu_\alpha(\mathbf{k}_u)} W_{(\mathbf{k}_u, \mathbf{0})}(\Phi_b(\mathbf{z})) \\
&= \frac{1}{b^m} \sum_{\mathbf{z} \in \mathcal{P}(\mathbf{q}, p)} \sum_{\emptyset \neq u \subseteq \{1, \dots, s\}} \prod_{j \in u} \gamma_j^{1/2} D_{\alpha, b}^{1/2} \sum_{k_j=1}^{\infty} b^{-\mu_\alpha(k_j)} W_{k_j}(\Phi_b(z_j)) \\
&= -1 + \frac{1}{b^m} \sum_{\mathbf{z} \in \mathcal{P}(\mathbf{q}, p)} \prod_{j=1}^s \left[ 1 + \gamma_j^{1/2} D_{\alpha, b}^{1/2} \chi_b \circ \Phi_b(z_j) \right],
\end{aligned}$$

where we define the function  $\chi_b : G \rightarrow \mathbb{R}$  by

$$\chi_b(z) := \sum_{k=1}^{\infty} b^{-\mu_\alpha(k)} W_k(z).$$

The difficulty in calculating  $B_\alpha(\mathbf{q}, p)$  lies in the fact that  $\chi_b(z)$  is expressed as an infinite sum over  $k \in \mathbb{N}$ . Under the assumption that  $z \in G$  is given in the form

$$(\zeta_1, \zeta_2, \dots, \zeta_n, 0, 0, \dots)^\top,$$

for  $n \in \mathbb{N}$  and  $\zeta_i \in \mathbb{Z}_b$ ,  $1 \leq i \leq n$ , it is possible to calculate  $\chi_b(z)$  in at most  $O(\alpha n)$  arithmetic operations as in [2, Theorem 2]. In the following we show that it is also possible to calculate  $\chi_b \circ \Phi_b(z)$  in at most  $O(\alpha n)$  arithmetic operations under the same assumption on  $z$ . Notice that this assumption on  $z$  is natural from Definition 13.

**Theorem 25.** *Let  $z \in G$  be given in the form  $(\zeta_1, \zeta_2, \dots, \zeta_n, 0, 0, \dots)^\top$  for  $n \in \mathbb{N}$  and  $\zeta_i \in \mathbb{Z}_b$ ,  $1 \leq i \leq n$ , that is,  $\zeta_{n+1} = \zeta_{n+2} = \dots = 0$ . Then  $\chi_b \circ \Phi_b(z)$  can be calculated as follows: we define the following vectors*

$$\begin{aligned}
\mathbf{U}(\zeta_1) &= (U_0(\zeta_1), U_1(\zeta_1), \dots, U_{\alpha-1}(\zeta_1)), \\
\tilde{\mathbf{U}}(\zeta_1) &= (\tilde{U}_0(\zeta_1), \tilde{U}_1(\zeta_1), \dots, \tilde{U}_{\alpha-1}(\zeta_1)), \\
\mathbf{V}(z) &= (V_1(z), \dots, V_{\alpha-1}(z)), \\
\tilde{\mathbf{V}}(z) &= (\tilde{V}_\alpha(z), \dots, \tilde{V}_1(z)),
\end{aligned}$$

where we set

$$\begin{aligned}
U_0(\zeta_1) &= 1, \\
U_t(\zeta_1) &= \frac{1}{b^{t(n-1)}} \prod_{i=1}^t \frac{\rho(\zeta_1)}{b^i - 1} \quad \text{for } 1 \leq t \leq \alpha - 1, \\
\tilde{U}_t(\zeta_1) &= \sum_{v=t}^{\alpha-1} U_{v-t}(\zeta_1) \quad \text{for } 0 \leq t \leq \alpha - 1,
\end{aligned}$$

where

$$\rho(\zeta_1) = \begin{cases} b-1 & \text{if } \zeta_1 = 0, \\ -1 & \text{otherwise.} \end{cases}$$

We further define

$$V_t(z) = \sum_{0 < a_t < \dots < a_1 < n} \prod_{i=1}^t b^{-a_i} L(z, a_i + 1),$$

$$\tilde{V}_t(z) = \sum_{0 < a_t < \dots < a_1 < n} b^{a_t-1} [\Phi_b(z) \in H_{a_t-1}] \prod_{i=1}^t b^{-a_i} L(z, a_i + 1),$$

for  $1 \leq t \leq \alpha-1$  and  $1 \leq t \leq \alpha$ , respectively. Here the value of  $[\Phi_b(z) \in H_{a_t-1}]$  equals 1 if  $\Phi_b(z) \in H_{a_t-1}$ , and 0 otherwise, where  $H_{a_t-1} := \{(\zeta'_1, \zeta'_2, \dots)^\top \in G : \zeta'_1 = \dots = \zeta'_{a_t-1} = 0\}$  for  $a_t \in \mathbb{N}$ . Furthermore,  $L(z, a_i + 1)$  is defined as

$$L(z, a_i + 1) := \begin{cases} b-1 & \text{if } \zeta_{a_i+1} = \zeta_1, \\ -1 & \text{if } \zeta_{a_i+1} \neq \zeta_1. \end{cases}$$

Using this notation, we have the following:

- If  $\zeta_1 = \dots = \zeta_n = 0$ ,

$$\chi_b \circ \Phi_b(z) = \sum_{v=1}^{\alpha-1} \prod_{i=1}^v \frac{b-1}{b^i-1} + \frac{b^\alpha-1}{b^\alpha-b} \prod_{i=1}^{\alpha} \frac{b-1}{b^i-1}.$$

- Otherwise,

$$\chi_b \circ \Phi_b(z) = \tilde{\mathbf{U}}_{1:\alpha-1}(\zeta_1) \cdot \mathbf{V}(z) + (\tilde{U}_0(\zeta_1) - 1) + \mathbf{U}(\zeta_1) \cdot \tilde{\mathbf{V}}(z),$$

where  $\mathbf{a} \cdot \mathbf{b}$  denotes the dot product and  $\tilde{\mathbf{U}}_{1:\alpha-1}(\zeta_1)$  is the vector of the last  $\alpha-1$  components of  $\tilde{\mathbf{U}}(\zeta_1)$ .

The proof of this theorem is given in Appendix B.

**Remark 26.** Note that  $V_t(z)$  and  $\tilde{V}_t(z)$  can be calculated as

$$V_t(z) = \sum_{a_1=t}^{n-1} b^{-a_1} L(z, a_1 + 1) \sum_{a_2=t-1}^{a_1-1} b^{-a_2} L(z, a_2 + 1) \dots \sum_{a_t=1}^{a_{t-1}-1} b^{-a_t} L(z, a_t + 1),$$

and

$$\begin{aligned} \tilde{V}_t(z) &= \sum_{a_1=t}^{n-1} b^{-a_1} L(z, a_1 + 1) \sum_{a_2=t-1}^{a_1-1} b^{-a_2} L(z, a_2 + 1) \\ &\quad \dots \sum_{a_t=1}^{a_{t-1}-1} b^{-1} [\Phi_b(z) \in H_{a_t-1}] L(z, a_t + 1), \end{aligned}$$

respectively. By using these forms, the vectors  $\mathbf{V}(z)$  and  $\tilde{\mathbf{V}}(z)$  can be computed in  $O(\alpha n)$  operations according to [2, Algorithm 4]. Thus the value of  $\chi_b \circ \Phi_b(z)$  can be computed in at most  $O(\alpha n)$  operations.

## 6.2 Fast component-by-component construction

We finally show how to obtain the fast CBC construction using the fast Fourier transform. Our exposition here follows basically along the same lines as [10, Subsection 6.2]. By denoting

$$P_{\tau-1}(h) := \prod_{j=1}^{\tau-1} \left[ 1 + \gamma_j^{1/2} D_{\alpha,b}^{1/2} \chi_b \circ \Phi_b \left( v_n \left( \frac{h(x)q_j(x)}{p(x)} \right) \right) \right],$$

and

$$Q(q, h) := \chi_b \circ \Phi_b \left( v_n \left( \frac{h(x)q(x)}{p(x)} \right) \right),$$

where the arguments  $h, q$  of  $P_{\tau-1}$  and  $Q$  are understood as integers, and  $P_0(h) = 1$  for any  $h \in \mathbb{N}_0$ , we have

$$\begin{aligned} & B_\alpha((\mathbf{q}_{\tau-1}, \tilde{q}_\tau), p) \\ &= -1 + \frac{1}{b^m} \sum_{\mathbf{z} \in \mathcal{P}((\mathbf{q}_{\tau-1}, \tilde{q}_\tau), p)} \prod_{j=1}^{\tau} \left[ 1 + \gamma_j^{1/2} D_{\alpha,b}^{1/2} \chi_b \circ \Phi_b(z_j) \right] \\ &= -1 + \frac{1}{b^m} \sum_{h=0}^{b^m-1} P_{\tau-1}(h) \left[ 1 + \gamma_\tau^{1/2} D_{\alpha,b}^{1/2} \chi_b \circ \Phi_b \left( v_n \left( \frac{h(x)\tilde{q}_\tau(x)}{p(x)} \right) \right) \right] \\ &= -1 + \frac{1}{b^m} \sum_{h=0}^{b^m-1} P_{\tau-1}(h) + \frac{\gamma_\tau^{1/2} D_{\alpha,b}^{1/2}}{b^m} \sum_{h=0}^{b^m-1} P_{\tau-1}(h) Q(\tilde{q}_\tau, h) \\ &= B_\alpha(\mathbf{q}_{\tau-1}, p) + \frac{\gamma_\tau^{1/2} D_{\alpha,b}^{1/2}}{b^m} \left[ P_{\tau-1}(0) Q(\tilde{q}_\tau, 0) + \sum_{h=1}^{b^m-1} P_{\tau-1}(h) Q(\tilde{q}_\tau, h) \right], \end{aligned}$$

where the argument  $\tilde{q}_\tau$  of  $Q$  is again understood as an integer. Since we have  $Q(q, 0) = \chi_b(0)$  for any  $q \in R_{b,n}$ , we can focus on the term

$$\sum_{h=1}^{b^m-1} P_{\tau-1}(h) Q(\tilde{q}_\tau, h), \quad (7)$$

and find  $\tilde{q}_\tau = q_\tau$  which minimizes (7) as a function of  $\tilde{q}_\tau \in R_{b,n}$  in Algorithm 22. Moreover, for  $\tilde{q}_\tau = 0$ , we have

$$\begin{aligned} B_\alpha((\mathbf{q}_{\tau-1}, 0), p) &= -1 + \frac{1}{b^m} \sum_{h=0}^{b^m-1} P_{\tau-1}(h) \left[ 1 + \gamma_\tau^{1/2} D_{\alpha,b}^{1/2} \chi_b(0) \right] \\ &= -\gamma_\tau^{1/2} D_{\alpha,b}^{1/2} \chi_b(0) + \left[ 1 + \gamma_\tau^{1/2} D_{\alpha,b}^{1/2} \chi_b(0) \right] B_\alpha(\mathbf{q}_{\tau-1}, p), \end{aligned}$$

which can be computed at a negligibly low cost, so that we only need to consider  $\tilde{q}_\tau \in R_{b,n} \setminus \{0\}$  in the following.

According to Algorithm 22, we choose an irreducible polynomial  $p \in \mathbb{Z}_b[x]$  with  $\deg(p) = n$ . Thus, there exists a primitive element  $g \in R_{b,n} \setminus \{0\}$ , which satisfies

$$\{g^0 \bmod p, g^1 \bmod p, \dots, g^{b^n-2} \bmod p\} = R_{b,n} \setminus \{0\},$$

and  $g^{-1} \bmod p = g^{b^n-2} \bmod p$ . Using this property of  $g$ , one can obtain the values of (7) for all  $\tilde{q}_\tau \in R_{b,n} \setminus \{0\}$  by a matrix-vector multiplication  $\mathbf{Q}_{\text{perm}} \mathbf{P}_{\tau-1}$ , where  $\mathbf{Q}_{\text{perm}}$  is a  $(b^n - 1) \times (b^m - 1)$  matrix given by permuting the rows of  $\mathbf{Q}$  as

$$\mathbf{Q}_{\text{perm}} := (Q(g^i \bmod p, h))_{0 \leq i \leq b^n-2, 0 < h < b^m},$$

and  $\mathbf{P}_{\tau-1}$  is a vector defined as

$$\mathbf{P}_{\tau-1} := (P_{\tau-1}(1), \dots, P_{\tau-1}(b^m - 1))^\top.$$

However, the multiplication  $\mathbf{Q}_{\text{perm}} \mathbf{P}_{\tau-1}$  requires  $O(b^{m+n})$  arithmetic operations, which can be reduced as follows.

As a first step, we add more columns to  $\mathbf{Q}_{\text{perm}}$  to obtain a  $(b^n - 1) \times (b^n - 1)$  matrix  $\mathbf{Q}'_{\text{perm}}$  given by

$$\mathbf{Q}'_{\text{perm}} := (Q(g^i \bmod p, h))_{0 \leq i \leq b^n-2, 0 < h < b^n}.$$

We also add more elements to  $\mathbf{P}_{\tau-1}$  to obtain a vector  $\mathbf{P}'_{\tau-1} = (\mathbf{P}_{\tau-1}^\top, \mathbf{0}^\top)^\top$ , where  $\mathbf{0}$  is the  $(b^n - b^m)$ -dimensional zero vector, such that we have  $\mathbf{Q}_{\text{perm}} \mathbf{P}_{\tau-1} = \mathbf{Q}'_{\text{perm}} \mathbf{P}'_{\tau-1}$ . Next we permute the rows of  $\mathbf{Q}'_{\text{perm}}$  to obtain a  $(b^n - 1) \times (b^n - 1)$  *circulant* matrix

$$\begin{aligned} \mathbf{Q}_{\text{circ}} &:= (Q(g^i \bmod p, g^{-h} \bmod p))_{0 \leq i, h \leq b^n-2} \\ &= \left( \chi_b \circ \Phi_b \left( v_n \left( \frac{(g^{i-h} \bmod p)(x)}{p(x)} \right) \right) \right)_{0 \leq i, h \leq b^n-2}, \end{aligned}$$

where the argument  $g^{-h} \bmod p$  of  $Q$  is again understood as an integer. Further, we introduce a vector  $\mathbf{R}_{\tau-1} = (R_{\tau-1}(0), \dots, R_{\tau-1}(b^n - 2))^\top$  such that

$$R_{\tau-1}(h) = \begin{cases} P_{\tau-1}(g^{-h} \bmod p) & \text{if } \deg(g^{-h} \bmod p) < m, \\ 0 & \text{otherwise,} \end{cases}$$

for  $0 \leq h \leq b^n - 2$ . Using these notations, we have  $\mathbf{Q}'_{\text{perm}} \mathbf{P}'_{\tau-1} = \mathbf{Q}_{\text{circ}} \mathbf{R}_{\tau-1}$ , which implies that a matrix-vector multiplication  $\mathbf{Q}_{\text{circ}} \mathbf{R}_{\tau-1}$  gives the values of (7) for all  $\tilde{q}_\tau \in R_{b,n} \setminus \{0\}$ . Since the matrix  $\mathbf{Q}_{\text{circ}}$  is circulant, the multiplication  $\mathbf{Q}_{\text{circ}} \mathbf{R}_{\tau-1}$  can be done efficiently by using the fast Fourier transform, requiring only  $O(nb^n)$  arithmetic operations [18]. This way we can reduce the cost from  $O(b^{m+n})$  to  $O(nb^n)$  operations for finding  $q_\tau \in R_{b,n}$  which minimizes  $B_\alpha((\mathbf{q}_{\tau-1}, \tilde{q}_\tau), p)$  as a function of  $\tilde{q}_\tau$ .

Suppose that  $g^i \bmod p \in R_{b,n} \setminus \{0\}$  minimizes  $B_\alpha((\mathbf{q}_{\tau-1}, \tilde{q}_\tau), p)$  as a function of  $\tilde{q}_\tau$ . We update  $\mathbf{R}_\tau$  by

$$R_\tau(h) = \begin{cases} R_{\tau-1}(h) \left[ 1 + \gamma_\tau^{1/2} D_{\alpha,b}^{1/2} Q(g^i \bmod p, g^{-h} \bmod p) \right] & \text{if } \deg(g^{-h} \bmod p) < m, \\ 0 & \text{otherwise,} \end{cases}$$

for  $0 \leq h \leq b^n - 2$ . We then move on to the next component. In summary, the fast CBC construction proceeds as follows.

1. Choose an irreducible polynomial  $p \in \mathbb{Z}_b[x]$  with  $\deg(p) = n$ .
2. Evaluate  $\mathbf{Q}_{\text{circ}}$  and  $\mathbf{R}_0$ .
3. For  $\tau = 1, \dots, s$ , do the following:
  - Compute the matrix-vector multiplication  $\mathbf{Q}_{\text{circ}}\mathbf{R}_{\tau-1}$  by using the fast Fourier transform.
  - Find  $q_\tau \in R_{b,n} \setminus \{0\}$  which gives the minimum value among the components of  $\mathbf{Q}_{\text{circ}}\mathbf{R}_{\tau-1}$ .
  - Update the vector  $\mathbf{R}_\tau$ .

In Step 2, since the matrix  $\mathbf{Q}_{\text{circ}}$  is circulant, we only need to evaluate one column of  $\mathbf{Q}_{\text{circ}}$ . Since one column consists of  $b^n - 1$  elements, each of which can be computed in at most  $O(\alpha n)$  operations as in Theorem 25, Step 2 can be done in at most  $O(\alpha n b^n)$  operations. The matrix-vector multiplication  $\mathbf{Q}_{\text{circ}}\mathbf{R}_{\tau-1}$  can be done in  $O(n b^n)$  operations and  $\mathbf{R}_\tau$  can be updated in  $O(b^n)$  operations, so that Step 3 can be done in  $O(s n b^n)$  operations. In total, the fast CBC construction can be done in  $O(s n b^n)$  operations. As for the required memory, we need to store one column of  $\mathbf{Q}_{\text{circ}}$  and  $\mathbf{R}_\tau$ , both of which require  $O(b^n)$  memory space.

We now recall that we can construct good FHOPLPs which achieve the optimal rate of the worst-case error when  $n \geq \alpha m/2$ , see Remark 24. Depending on whether  $\alpha m$  is even or odd, we may choose  $n = \alpha m/2$  or  $n = (\alpha m + 1)/2$ , respectively. In both cases, the computational cost of the fast CBC construction becomes  $O(s \alpha m b^{\alpha m/2}) = O(s \alpha N^{\alpha/2} \log N)$  operations using  $O(b^{\alpha m/2}) = O(N^{\alpha/2})$  memory.

**Remark 27.** In [13], the authors studied the mean square worst-case error of digitally shifted and then folded higher order polynomial lattice point sets in the same function space  $\mathcal{H}_\alpha$  and proved the existence of good higher order polynomial lattice rules which achieve the optimal convergence rate. Following an argument similar to the previous section, it is possible to prove that the CBC construction can find good higher order polynomial lattice rules which achieve the optimal convergence rate. Moreover, the fast CBC construction can also be obtained by slightly modifying the argument of this section.

## A Proof of Theorem 23

In order to prove Theorem 23, we need the following lemma, see [13, Lemma 25] for the proof.

**Lemma 28.** Let  $b$  be a prime, let  $\alpha \geq 2$  be an integer. For  $n \in \mathbb{N}$  and a real number  $\lambda > 1/\alpha$ , we have

$$\sum_{k \in \mathcal{E}} b^{-\lambda \mu_\alpha(\lfloor k/b \rfloor)} \leq A_{\alpha,b,\lambda,1} \quad \text{and} \quad \sum_{\substack{k \in \mathcal{E} \\ b^n | k}} b^{-\lambda \mu_\alpha(\lfloor k/b \rfloor)} \leq \frac{A_{\alpha,b,\lambda,2}}{b^{2\lambda n}},$$

where  $A_{\alpha,b,\lambda,1}$  and  $A_{\alpha,b,\lambda,2}$  are positive and depend only on  $\alpha$ ,  $b$  and  $\lambda$ , which are respectively given by

$$A_{\alpha,b,\lambda,1} = \frac{b}{b-1} \left[ \sum_{v=1}^{\alpha-1} \prod_{i=1}^v \left( \frac{b-1}{b^{\lambda i} - 1} \right) + \frac{b^{\lambda\alpha} - 1}{b^{\lambda\alpha} - b} \prod_{i=1}^{\alpha} \left( \frac{b-1}{b^{\lambda i} - 1} \right) \right],$$

and

$$A_{\alpha,b,\lambda,2} = \frac{1}{b-1} \sum_{v=2}^{\alpha-1} \prod_{i=1}^v \left( \frac{b^{\lambda}(b-1)}{b^{\lambda i} - 1} \right) + \frac{b^{\lambda}}{b^{\lambda\alpha} - b} \prod_{i=1}^{\alpha-1} \left( \frac{b^{\lambda}(b-1)}{b^{\lambda i} - 1} \right).$$

Here we note that  $A_{\alpha,b,\lambda}$  in Theorem 23 is given by  $A_{\alpha,b,\lambda} = A_{\alpha,b,\lambda,1} + A_{\alpha,b,\lambda,2}$ . In the following argument, we shall use the inequality

$$\left( \sum_n a_n \right)^\lambda \leq \sum_n a_n^\lambda, \quad (8)$$

for any sequence of non-negative real numbers  $(a_n)_{n \in \mathbb{N}}$  and any  $0 < \lambda \leq 1$ .

We now prove Theorem 23 by induction. Let us consider the case  $\tau = 1$  first. There exists at least one polynomial  $q_1 \in R_{b,n}$  for which  $B_\alpha^\lambda(q_1, p)$  is smaller than or equal to the average of  $B_\alpha^\lambda(\tilde{q}_1, p)$  over  $\tilde{q}_1 \in R_{b,n}$ . Thus, we have

$$\begin{aligned} B_\alpha^\lambda(q_1, p) &\leq \frac{1}{b^n} \sum_{\tilde{q}_1 \in R_{b,n}} B_\alpha^\lambda(\tilde{q}_1, p) \\ &\leq \gamma_1^{\lambda/2} D_{\alpha,b}^{\lambda/2} \sum_{k_1 \in \mathcal{E}} b^{-\lambda\mu_\alpha(\lfloor k_1/b \rfloor)} \frac{1}{b^n} \sum_{\substack{\tilde{q}_1 \in R_{b,n} \\ \text{tr}_n(k_1) \cdot \tilde{q}_1 \equiv a \pmod{p} \\ \deg(a) < n-m}} 1, \end{aligned} \quad (9)$$

for  $0 < \lambda \leq 1$ . The innermost sum equals the number of solutions  $\tilde{q}_1 \in R_{b,n}$  such that  $\text{tr}_n(k_1) \cdot \tilde{q}_1 \equiv a \pmod{p}$  with  $\deg(a) < n - m$ . If  $\text{tr}_n(k_1)$  is a multiple of  $p$ , we have  $\text{tr}_n(k_1) \cdot \tilde{q}_1 \equiv 0 \pmod{p}$  independently of  $\tilde{q}_1$ , so that we have

$$\frac{1}{b^n} \sum_{\substack{\tilde{q}_1 \in R_{b,n} \\ \text{tr}_n(k_1) \cdot \tilde{q}_1 \equiv a \pmod{p} \\ \deg(a) < n-m}} 1 = 1.$$

Otherwise if  $\text{tr}_n(k_1)$  is not a multiple of  $p$ , then there are  $b^{n-m}$  possible choices for  $a \in \mathbb{Z}_b[x]$  such that  $\deg(a) < n - m$ , for each of which there is one solution  $\tilde{q}_1$  to  $\text{tr}_n(k_1) \cdot \tilde{q}_1 \equiv a \pmod{p}$ , so that we have

$$\frac{1}{b^n} \sum_{\substack{\tilde{q}_1 \in R_{b,n} \\ \text{tr}_n(k_1) \cdot \tilde{q}_1 \equiv a \pmod{p} \\ \deg(a) < n-m}} 1 = \frac{1}{b^m}.$$

Substituting these results into (9) and using Lemma 28, we obtain

$$B_\alpha^\lambda(q_1, p) \leq \gamma_1^{\lambda/2} D_{\alpha,b}^{\lambda/2} \left( \sum_{\substack{k_1 \in \mathcal{E} \\ b^n | k_1}} b^{-\lambda\mu_\alpha(\lfloor k_1/b \rfloor)} + \frac{1}{b^m} \sum_{\substack{k_1 \in \mathcal{E} \\ b^n \nmid k_1}} b^{-\lambda\mu_\alpha(\lfloor k_1/b \rfloor)} \right)$$

$$\begin{aligned}
&\leq \gamma_1^{\lambda/2} D_{\alpha,b}^{\lambda/2} \left( \frac{A_{\alpha,b,\lambda,2}}{b^{2\lambda n}} + \frac{A_{\alpha,b,\lambda,1}}{b^m} \right) \\
&\leq \frac{\gamma_1^{\lambda/2} D_{\alpha,b}^{\lambda/2}}{b^{\min(m, 2\lambda n)}} (A_{\alpha,b,\lambda,1} + A_{\alpha,b,\lambda,2}) = \frac{\gamma_1^{\lambda/2} D_{\alpha,b}^{\lambda/2} A_{\alpha,b,\lambda}}{b^{\min(m, 2\lambda n)}},
\end{aligned}$$

for  $1/\alpha < \lambda \leq 1$ . Hence the result for the case  $\tau = 1$  follows.

Next we suppose that for  $1 \leq \tau < s$ , the inequality

$$B_\alpha(\mathbf{q}_\tau, p) \leq \frac{1}{b^{\min(m/\lambda, 2n)}} \left[ -1 + \prod_{j=1}^{\tau} \left( 1 + \gamma_j^{\lambda/2} D_{\alpha,b}^{\lambda/2} A_{\alpha,b,\lambda} \right) \right]^{1/\lambda} \quad (10)$$

holds true for any  $1/\alpha < \lambda \leq 1$ . Then we have

$$\begin{aligned}
&B_\alpha((\mathbf{q}_\tau, \tilde{q}_{\tau+1}), p) \\
&= \sum_{\emptyset \neq u \subseteq \{1, \dots, \tau+1\}} \gamma_u^{1/2} D_{\alpha,b}^{|u|/2} \sum_{\substack{\mathbf{k}_u \in \mathcal{E}^{|u|} \\ (\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}^\perp((\mathbf{q}_\tau, \tilde{q}_{\tau+1}), p)}} b^{-\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor)} \\
&= \sum_{\emptyset \neq u \subseteq \{1, \dots, \tau\}} \gamma_u^{1/2} D_{\alpha,b}^{|u|/2} \sum_{\substack{\mathbf{k}_u \in \mathcal{E}^{|u|} \\ (\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}^\perp((\mathbf{q}_\tau, \tilde{q}_{\tau+1}), p)}} b^{-\mu_\alpha(\lfloor \mathbf{k}_u/b \rfloor)} \\
&\quad + \sum_{u \subseteq \{1, \dots, \tau\}} \gamma_{u \cup \{\tau+1\}}^{1/2} D_{\alpha,b}^{(|u|+1)/2} \sum_{\substack{\mathbf{k}_{u \cup \{\tau+1\}} \in \mathcal{E}^{|u|+1} \\ (\mathbf{k}_{u \cup \{\tau+1\}}, \mathbf{0}) \in \mathcal{P}^\perp((\mathbf{q}_\tau, \tilde{q}_{\tau+1}), p)}} b^{-\mu_\alpha(\lfloor \mathbf{k}_{u \cup \{\tau+1\}}/b \rfloor)} \\
&=: B_\alpha(\mathbf{q}_\tau, p) + \theta(\mathbf{q}_\tau, \tilde{q}_{\tau+1}, p), \quad (11)
\end{aligned}$$

where we denote by  $\theta(\mathbf{q}_\tau, \tilde{q}_{\tau+1}, p)$  the second term in the last equality. In Algorithm 22, we choose  $q_{\tau+1} \in R_{b,n}$  which minimizes  $\theta(\mathbf{q}_\tau, \tilde{q}_{\tau+1}, p)$  as a function of  $\tilde{q}_{\tau+1}$ , since the dependence of  $B_\alpha((\mathbf{q}_\tau, \tilde{q}_{\tau+1}), p)$  on  $\tilde{q}_{\tau+1}$  appears only in  $\theta(\mathbf{q}_\tau, \tilde{q}_{\tau+1}, p)$ . Using an averaging argument and the inequality (8), we have

$$\begin{aligned}
\theta^\lambda(\mathbf{q}_\tau, q_{\tau+1}, p) &\leq \frac{1}{b^n} \sum_{\tilde{q}_{\tau+1} \in R_{b,n}} \theta^\lambda(\mathbf{q}_\tau, \tilde{q}_{\tau+1}, p) \\
&\leq \sum_{u \subseteq \{1, \dots, \tau\}} \gamma_{u \cup \{\tau+1\}}^{\lambda/2} D_{\alpha,b}^{\lambda(|u|+1)/2} \sum_{\mathbf{k}_{u \cup \{\tau+1\}} \in \mathcal{E}^{|u|+1}} b^{-\lambda \mu_\alpha(\lfloor \mathbf{k}_{u \cup \{\tau+1\}}/b \rfloor)} \\
&\quad \times \frac{1}{b^n} \sum_{\substack{\tilde{q}_{\tau+1} \in R_{b,n} \\ \text{tr}_n(\mathbf{k}_u) \cdot \mathbf{q}_u + \text{tr}_n(k_{\tau+1}) \cdot \tilde{q}_{\tau+1} \equiv a \pmod{p} \\ \deg(a) < n-m}} 1,
\end{aligned}$$

for  $0 < \lambda \leq 1$ . If  $\text{tr}_n(k_{\tau+1})$  is a multiple of  $p$ , then we have

$$\text{tr}_n(\mathbf{k}_u) \cdot \mathbf{q}_u + \text{tr}_n(k_{\tau+1}) \cdot \tilde{q}_{\tau+1} \equiv \text{tr}_n(\mathbf{k}_u) \cdot \mathbf{q}_u \pmod{p},$$

so that the innermost sum equals  $b^n$  for  $(\mathbf{k}_u, \mathbf{0}) \in \mathcal{P}^\perp(\mathbf{q}_\tau, p)$ , and equals 0 otherwise. If  $\text{tr}_n(k_{\tau+1})$  is not a multiple of  $p$ , there are  $b^{n-m}$  possible choices for  $a$  such that  $\deg(a) < n-m$ , for each of which there exists at most one solution  $\tilde{q}_{\tau+1}$  to  $\text{tr}_n(k_{\tau+1}) \cdot \tilde{q}_{\tau+1} \equiv a - \text{tr}_n(\mathbf{k}_u) \cdot \mathbf{q}_u \pmod{p}$ , so that the innermost sum is bounded above by  $b^{n-m}$ . From these results and using Lemma 28, we have

$$\theta^\lambda(\mathbf{q}_\tau, q_{\tau+1}, p)$$



$$\begin{aligned}
&\leq \sum_{u \subseteq \{1, \dots, \tau\}} \gamma_{u \cup \{\tau+1\}}^{\lambda/2} D_{\alpha, b}^{\lambda(|u|+1)/2} \sum_{\substack{\mathbf{k}_{u \cup \{\tau+1\}} \in \mathcal{E}^{|u|+1} \\ b^n |k_{\tau+1}}} b^{-\lambda \mu_\alpha(\lfloor \mathbf{k}_{u \cup \{\tau+1\}} / b \rfloor)} \\
&\quad + \frac{1}{b^m} \sum_{u \subseteq \{1, \dots, \tau\}} \gamma_{u \cup \{\tau+1\}}^{\lambda/2} D_{\alpha, b}^{\lambda(|u|+1)/2} \sum_{\substack{\mathbf{k}_{u \cup \{\tau+1\}} \in \mathcal{E}^{|u|+1} \\ b^n \nmid k_{\tau+1}}} b^{-\lambda \mu_\alpha(\lfloor \mathbf{k}_{u \cup \{\tau+1\}} / b \rfloor)} \\
&\leq \sum_{u \subseteq \{1, \dots, \tau\}} \gamma_{u \cup \{\tau+1\}}^{\lambda/2} D_{\alpha, b}^{\lambda(|u|+1)/2} \sum_{\mathbf{k}_u \in \mathcal{E}^{|u|}} b^{-\lambda \mu_\alpha(\lfloor \mathbf{k}_u / b \rfloor)} \\
&\quad \times \left( \sum_{\substack{k_{\tau+1} \in \mathcal{E} \\ b^n |k_{\tau+1}}} b^{-\lambda \mu_\alpha(\lfloor k_{\tau+1} / b \rfloor)} + \frac{1}{b^m} \sum_{k_{\tau+1} \in \mathcal{E}} b^{-\lambda \mu_\alpha(\lfloor k_{\tau+1} / b \rfloor)} \right) \\
&\leq \sum_{u \subseteq \{1, \dots, \tau\}} \gamma_{u \cup \{\tau+1\}}^{\lambda/2} D_{\alpha, b}^{\lambda(|u|+1)/2} A_{\alpha, b, \lambda, 1}^{|u|} \left( \frac{A_{\alpha, b, \lambda, 2}}{b^{2\lambda n}} + \frac{A_{\alpha, b, \lambda, 1}}{b^m} \right) \\
&\leq \frac{\gamma_{\tau+1}^{\lambda/2} D_{\alpha, b}^{\lambda/2} A_{\alpha, b, \lambda}}{b^{\min(m, 2\lambda n)}} \sum_{u \subseteq \{1, \dots, \tau\}} \gamma_u^{\lambda/2} D_{\alpha, b}^{\lambda|u|/2} A_{\alpha, b, \lambda}^{|u|} \\
&= \frac{\gamma_{\tau+1}^{\lambda/2} D_{\alpha, b}^{\lambda/2} A_{\alpha, b, \lambda}}{b^{\min(m, 2\lambda n)}} \prod_{j=1}^{\tau} \left( 1 + \gamma_j^{\lambda/2} D_{\alpha, b}^{\lambda/2} A_{\alpha, b, \lambda} \right), \tag{12}
\end{aligned}$$

for  $1/\alpha < \lambda \leq 1$ . Applying the inequality (8) to (11) in which  $q_{\tau+1}$  equals that  $\tilde{q}_{\tau+1}$  which minimizes  $\theta^\lambda(\mathbf{q}_\tau, \tilde{q}_{\tau+1}, p)$ , and then using (10) and (12), we obtain

$$\begin{aligned}
B_\alpha^\lambda(\mathbf{q}_{\tau+1}, p) &\leq B_\alpha^\lambda(\mathbf{q}_\tau, p) + \theta^\lambda(\mathbf{q}_\tau, q_{\tau+1}, p) \\
&\leq \frac{1}{b^{\min(m, 2\lambda n)}} \left[ -1 + \prod_{j=1}^{\tau} \left( 1 + \gamma_j^{\lambda/2} D_{\alpha, b}^{\lambda/2} A_{\alpha, b, \lambda} \right) \right] \\
&\quad + \frac{\gamma_{\tau+1}^{\lambda/2} D_{\alpha, b}^{\lambda/2} A_{\alpha, b, \lambda}}{b^{\min(m, 2\lambda n)}} \prod_{j=1}^{\tau} \left( 1 + \gamma_j^{\lambda/2} D_{\alpha, b}^{\lambda/2} A_{\alpha, b, \lambda} \right) \\
&= \frac{1}{b^{\min(m, 2\lambda n)}} \left[ -1 + \prod_{j=1}^{\tau+1} \left( 1 + \gamma_j^{\lambda/2} D_{\alpha, b}^{\lambda/2} A_{\alpha, b, \lambda} \right) \right],
\end{aligned}$$

for  $1/\alpha < \lambda \leq 1$ , which completes the proof.

## B Proof of Theorem 25

Since  $z \in G$  is given in the form  $(\zeta_1, \zeta_2, \dots, \zeta_n, 0, 0, \dots)^\top$  for  $n \in \mathbb{N}$  and  $\zeta_i \in \mathbb{Z}_b$ ,  $1 \leq i \leq n$ ,  $\Phi_b(z)$  is given as

$$\Phi_b(z) = (\eta_1, \eta_2, \dots)^\top \in G \quad \text{with} \quad \eta_i = \zeta_{i+1} - \zeta_1 \pmod{b},$$

where  $\zeta_{n+1} = \zeta_{n+2} = \dots = 0$ .

Let us consider the first part. If  $\zeta_1 = \dots = \zeta_n = 0$ , it holds that  $\Phi_b(z) =$

$(0, 0, \dots)^\top$ , and thus,  $W_k(\Phi_b(z)) = 1$  for all  $k \in \mathbb{N}$ . Therefore, we have

$$\chi_b \circ \Phi_b(z) = \sum_{k=1}^{\infty} b^{-\mu_\alpha(k)},$$

where the result of the last sum is given in [2, Theorem 2], which proves the first part.

Let us consider the second part next. We denote the  $b$ -adic expansion of  $k \in \mathbb{N}$  by  $k = \kappa_1 b^{a_1-1} + \dots + \kappa_v b^{a_v-1}$  for some  $v \in \mathbb{N}$  such that  $a_1 > \dots > a_v > 0$  and  $0 < \kappa_1, \dots, \kappa_v < b$ . Then we have  $\mu_\alpha(k) = a_1 + \dots + a_{\min(v, \alpha)}$  and

$$W_k(\Phi_b(z)) = \prod_{i=1}^v \omega_b^{\kappa_i(\zeta_{a_i+1}-\zeta_1)}.$$

Here we note that  $\mu_\alpha(k)$  does not depend on the values of  $\kappa_1, \dots, \kappa_v$ . Using this result and arranging every element of  $\mathbb{N}$  according to the value of  $v$  in their expansions, we obtain

$$\begin{aligned} & \chi_b \circ \Phi_b(z) \\ &= \sum_{v=1}^{\infty} \sum_{0 < a_v < \dots < a_1} b^{-\sum_{i=1}^{\min(v, \alpha)} a_i} \sum_{0 < \kappa_1, \dots, \kappa_v < b} \prod_{i=1}^v \omega_b^{\kappa_i(\zeta_{a_i+1}-\zeta_1)} \\ &= \sum_{v=1}^{\alpha-1} \sum_{0 < a_v < \dots < a_1} \prod_{i=1}^v \left( b^{-a_i} \sum_{\kappa_i=1}^{b-1} \omega_b^{\kappa_i(\zeta_{a_i+1}-\zeta_1)} \right) \\ & \quad + \sum_{v=\alpha}^{\infty} \sum_{0 < a_v < \dots < a_1} \prod_{i=1}^{\alpha} \left( b^{-a_i} \sum_{\kappa_i=1}^{b-1} \omega_b^{\kappa_i(\zeta_{a_i+1}-\zeta_1)} \right) \prod_{j=\alpha+1}^v \left( \sum_{\kappa_j=1}^{b-1} \omega_b^{\kappa_j(\zeta_{a_j+1}-\zeta_1)} \right), \end{aligned} \tag{13}$$

wherein we have

$$\begin{aligned} \sum_{\kappa_i=1}^{b-1} \omega_b^{\kappa_i(\zeta_{a_i+1}-\zeta_1)} &= \begin{cases} b-1 & (\zeta_{a_i+1} - \zeta_1 = 0) \\ -1 & (\zeta_{a_i+1} - \zeta_1 \neq 0) \end{cases} \\ &= L(z, a_i + 1). \end{aligned}$$

Thus, the second term on the right-hand side of (13) becomes

$$\begin{aligned} & \sum_{v=\alpha}^{\infty} \sum_{0 < a_v < \dots < a_1} \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \prod_{j=\alpha+1}^v L(z, a_j + 1) \\ &= \sum_{0 < a_\alpha < \dots < a_1} \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \\ & \quad \times \sum_{v=\alpha}^{\infty} \sum_{0 < a_v < \dots < a_{\alpha+1} < a_\alpha} \prod_{i' \in \{a_v, \dots, a_{\alpha+1}\}} L(z, i' + 1) \prod_{i'' \in \{1, \dots, a_\alpha-1\} \setminus \{a_v, \dots, a_{\alpha+1}\}} 1 \\ &= \sum_{0 < a_\alpha < \dots < a_1} \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \sum_{u \subseteq \{1, \dots, a_\alpha-1\}} \prod_{i' \in u} L(z, i' + 1) \prod_{i'' \in \{1, \dots, a_\alpha-1\} \setminus u} 1 \end{aligned}$$

$$= \sum_{0 < a_\alpha < \dots < a_1} \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \prod_{j=1}^{a_\alpha - 1} [1 + L(z, j + 1)]. \quad (14)$$

The innermost product equals  $b^{a_\alpha - 1}$  if and only if  $L(z, j + 1) = b - 1$  for all  $1 \leq j < a_\alpha$  and equals 0 otherwise. Since  $L(z, j + 1) = b - 1$  only when  $\zeta_{j+1} = \zeta_1$ , we focus on the condition  $\zeta_{j+1} = \zeta_1$  for all  $1 \leq j < a_\alpha$ . It is obvious that  $z \in G$  satisfying this condition can be expressed in the form

$$(\underbrace{\zeta_1, \zeta_1, \dots, \zeta_1}_{a_\alpha}, \zeta_{a_\alpha+1}, \zeta_{a_\alpha+2}, \dots)^\top.$$

For such  $z$  we have

$$\Phi_b(z) = (\underbrace{0, 0, \dots, 0}_{a_\alpha - 1}, \eta_{a_\alpha+1}, \eta_{a_\alpha+2}, \dots)^\top.$$

Therefore, the innermost product on the right-most side of (14) equals  $b^{a_\alpha - 1}$  if  $\Phi_b(z) \in H_{a_\alpha - 1}$ , and equals 0 otherwise. Hence the second term on the right-hand side of (13) can be further rewritten as

$$\sum_{0 < a_\alpha < \dots < a_1} b^{a_\alpha - 1} [\Phi_b(z) \in H_{a_\alpha - 1}] \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1).$$

Substituting this result into (13) we have

$$\begin{aligned} \chi_b \circ \Phi_b(z) &= \sum_{v=1}^{\alpha-1} \sum_{0 < a_v < \dots < a_1} \prod_{i=1}^v b^{-a_i} L(z, a_i + 1) \\ &\quad + \sum_{0 < a_\alpha < \dots < a_1} b^{a_\alpha - 1} [\Phi_b(z) \in H_{a_\alpha - 1}] \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1). \end{aligned} \quad (15)$$

For the first term on the right-hand side of (15) we have

$$\begin{aligned} &\sum_{0 < a_v < \dots < a_1} \prod_{i=1}^v b^{-a_i} L(z, a_i + 1) \\ &= \sum_{0 < a_v < \dots < a_1 < n} \prod_{i=1}^v b^{-a_i} L(z, a_i + 1) + \sum_{0 < a_v < \dots < a_2 < n \leq a_1} \prod_{i=1}^v b^{-a_i} L(z, a_i + 1) \\ &\quad + \dots + \sum_{0 < a_v < n \leq a_{v-1} < \dots < a_1} \prod_{i=1}^v b^{-a_i} L(z, a_i + 1) + \sum_{n \leq a_v < \dots < a_1} \prod_{i=1}^v b^{-a_i} L(z, a_i + 1) \\ &= \sum_{t=0}^v \sum_{0 < a_v < \dots < a_{t+1} < n} \prod_{i=t+1}^v b^{-a_i} L(z, a_i + 1) \sum_{n \leq a_t < \dots < a_1} \prod_{j=1}^t b^{-a_j} L(z, a_j + 1), \\ &= \sum_{t=0}^v V_{v-t}(z) \sum_{n \leq a_t < \dots < a_1} \prod_{j=1}^t b^{-a_j} L(z, a_j + 1), \end{aligned}$$

where we define  $V_0(z) = 1$  for any  $z \in G$ . We now recall that  $z \in G$  is given in the form  $(\zeta_1, \zeta_2, \dots, \zeta_n, 0, 0, \dots)^\top$  for  $n \in \mathbb{N}$  and  $\zeta_i \in \mathbb{Z}_b$ ,  $1 \leq i \leq n$ . From this

assumption, we have  $\zeta_{n+1} = \zeta_{n+2} = \dots = 0$ , so that for any  $i \geq n$

$$\begin{aligned} L(z, i+1) &= \begin{cases} b-1 & (\zeta_1 = 0) \\ -1 & (\zeta_1 \neq 0) \end{cases} \\ &= \rho(\zeta_1). \end{aligned}$$

Therefore in the last expression we have

$$\begin{aligned} \sum_{n \leq a_t < \dots < a_1} \prod_{j=1}^t b^{-a_j} L(z, a_j + 1) &= \rho^t(\zeta_1) \sum_{n \leq a_t < \dots < a_1} \prod_{j=1}^t b^{-a_j} \\ &= \rho^t(\zeta_1) \sum_{a_t=n}^{\infty} b^{-a_t} \sum_{a_{t-1}=a_t+1}^{\infty} b^{-a_{t-1}} \dots \sum_{a_1=a_2+1}^{\infty} b^{-a_1} \\ &= \frac{1}{b^{t(n-1)}} \prod_{i=1}^t \frac{\rho(\zeta_1)}{b^i - 1} = U_t(\zeta_1). \end{aligned} \quad (16)$$

Using these results and swapping the order of sums, the first term on the right-hand side of (15) becomes

$$\begin{aligned} \sum_{v=1}^{\alpha-1} \sum_{0 < a_v < \dots < a_1} \prod_{i=1}^v b^{-a_i} L(z, a_i + 1) &= \sum_{v=1}^{\alpha-1} \sum_{t=0}^v V_{v-t}(z) U_t(\zeta_1) \\ &= \sum_{t=1}^{\alpha-1} \left( \sum_{v=t}^{\alpha-1} U_{v-t}(\zeta_1) \right) V_t(z) + \sum_{v=1}^{\alpha-1} U_v(\zeta_1) \\ &= \sum_{t=1}^{\alpha-1} \tilde{U}_t(\zeta_1) V_t(z) + (\tilde{U}_0(\zeta_1) - 1). \end{aligned}$$

For the second term on the right-hand side of (15), we have

$$\begin{aligned} &\sum_{0 < a_\alpha < \dots < a_1} b^{a_\alpha-1} [\Phi_b(z) \in H_{a_\alpha-1}] \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \\ &= \sum_{0 < a_\alpha < \dots < a_1 < n} b^{a_\alpha-1} [\Phi_b(z) \in H_{a_\alpha-1}] \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \\ &\quad + \sum_{0 < a_\alpha < \dots < a_2 < n \leq a_1} b^{a_\alpha-1} [\Phi_b(z) \in H_{a_\alpha-1}] \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \\ &\quad + \dots + \sum_{n \leq a_\alpha < \dots < a_1} b^{a_\alpha-1} [\Phi_b(z) \in H_{a_\alpha-1}] \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \\ &= \sum_{t=0}^{\alpha} \sum_{0 < a_\alpha < \dots < a_{t+1} < n} b^{a_\alpha-1} [\Phi_b(z) \in H_{a_\alpha-1}] \prod_{i=t+1}^{\alpha} b^{-a_i} L(z, a_i + 1) \\ &\quad \times \sum_{n \leq a_t < \dots < a_1} \prod_{j=1}^t b^{-a_j} L(z, a_j + 1). \end{aligned}$$

Here again we recall that  $z \in G$  is given in the form  $(\zeta_1, \zeta_2, \dots, \zeta_n, 0, 0, \dots)^\top$  for  $n \in \mathbb{N}$  and  $\zeta_i \in \mathbb{Z}_b$ ,  $1 \leq i \leq n$ . Furthermore, it does not hold that  $\zeta_1 = \dots =$

$\zeta_n = 0$  for the second part of this theorem. Therefore,  $\Phi_b(z) \notin H_{a_\alpha-1}$  whenever  $a_\alpha \geq n$ . Thus, we have

$$\sum_{n \leq a_\alpha < \dots < a_1} b^{a_\alpha-1} [\Phi_b(z) \in H_{a_\alpha-1}] \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) = 0.$$

Thus, by using the above result and (16), the second term on the right-hand side of (15) becomes

$$\begin{aligned} & \sum_{0 < a_\alpha < \dots < a_1} b^{a_\alpha-1} [\Phi_b(z) \in H_{a_\alpha-1}] \prod_{i=1}^{\alpha} b^{-a_i} L(z, a_i + 1) \\ &= \sum_{t=0}^{\alpha-1} \tilde{V}_{\alpha-t}(z) U_t(\zeta_1) = \sum_{t=1}^{\alpha} U_{\alpha-t}(\zeta_1) \tilde{V}_t(z). \end{aligned}$$

Therefore, we have

$$\chi_b \circ \Phi_b(z) = \sum_{t=1}^{\alpha-1} \tilde{U}_t(\zeta_1) V_t(z) + (\tilde{U}_0(\zeta_1) - 1) + \sum_{t=1}^{\alpha} U_{\alpha-t}(\zeta_1) \tilde{V}_t(z),$$

which completes the proof of the second part.

## References

- [1] J. Baldeaux and J. Dick, QMC rules of arbitrary high order: reproducing kernel Hilbert space approach, *Constr. Approx.*, 30 (2009) 495–527.
- [2] J. Baldeaux, J. Dick, G. Leobacher, D. Nuyens and F. Pillichshammer, Efficient calculation of the worst-case error and (fast) component-by-component construction of higher order polynomial lattice rules, *Numer. Algorithms*, 59 (2012) 403–431.
- [3] L. L. Cristea, J. Dick, G. Leobacher and F. Pillichshammer, The tent transformation can improve the convergence rate of quasi-Monte Carlo algorithms using digital nets, *Numer. Math.*, 105 (2007) 413–455.
- [4] J. Dick, Walsh spaces containing smooth functions and quasi-Monte Carlo rules of arbitrary high order, *SIAM J. Numer. Anal.*, 46 (2008) 1519–1553.
- [5] J. Dick, F. Y. Kuo, Q. T. Le Qia, D. Nuyens and C. Schwab, Higher order QMC Petrov–Galerkin discretization for affine parametric operator equations with random field inputs, *SIAM J. Numer. Anal.*, 52 (2014) 2676–2702.
- [6] J. Dick and M. Matsumoto, On the fast computation of the weight enumerator polynomial and the  $t$  value of digital nets over finite abelian groups, *SIAM J. Discrete Math.*, 27 (2013) 1335–1359.
- [7] J. Dick and F. Pillichshammer, Strong tractability of multivariate integration of arbitrary high order using digitally shifted polynomial lattice rules, *J. Complexity*, 23 (2007) 436–453.

- [8] J. Dick and F. Pillichshammer, *Digital nets and sequences. Discrepancy theory and quasi-Monte Carlo integration*, Cambridge University Press, Cambridge, 2010.
- [9] T. Goda, On the  $L_p$  discrepancy of two-dimensional folded Hammersley point sets, *Arch. Math.*, 103 (2014) 389–398.
- [10] T. Goda, Constructing good higher order polynomial lattice rules with modulus of reduced degree, *J. Complexity*, 31 (2015) 237–259.
- [11] T. Goda, Good interlaced polynomial lattice rules for numerical integration in weighted Walsh spaces, *J. Comput. Appl. Math.*, 285 (2015) 279–294.
- [12] T. Goda and J. Dick, Construction of interlaced scrambled polynomial lattice rules of arbitrary high order, *Found. Comput. Math.*, (in press) <http://dx.doi.org/10.1007/s10208-014-9226-8>.
- [13] T. Goda, K. Suzuki and T. Yoshiki, The  $b$ -adic tent transformation for quasi-Monte Carlo integration using digital nets, *J. Approx. Theory*, 194 (2015) 62–86.
- [14] F. J. Hickernell, Obtaining  $O(N^{-2+\epsilon})$  convergence for lattice quadrature rules, In: K.-T. Fang, F. J. Hickernell, H. Niederreiter (eds.) *Monte Carlo and Quasi-Monte Carlo Methods 2000*, pp. 274–289. Springer, Berlin, 2002.
- [15] H. Niederreiter, Low-discrepancy point sets obtained by digital constructions over finite fields, *Czechoslovak Math. J.*, 42 (1992) 143–166.
- [16] H. Niederreiter, *Random number generation and quasi-Monte Carlo methods*, CBMS-NSF Series in Applied Mathematics, vol. 63, SIAM, Philadelphia, 1992.
- [17] H. Niederreiter and C. P. Xing, *Rational points on curves over finite fields. Theory and applications*, London Mathematical Society Lecture Note Series vol. 285, Cambridge University Press, Cambridge, 2001.
- [18] D. Nuyens and R. Cools, Fast component-by-component construction, a reprise for different kernels, In: *Monte Carlo and Quasi-Monte Carlo Methods 2004*, pp. 373–387, Springer, Berlin, 2006.
- [19] L. S. Pontryagin, *Topological groups*, Translated from the second Russian edition by Arlen Brown, Gordon and Breach Science Publishers, Inc., New York-London-Paris, 1966.
- [20] I. F. Sharygin, A lower estimate for the error of quadrature formulas for certain classes of functions, *Zh. Vychisl. Mat. i Mat. Fiz.*, 3 (1963) 370–376.
- [21] F. SCHIPP, W. R. WADE AND P. SIMON, *Walsh series: An introduction to dyadic harmonic analysis*, Adam Hilger, Bristol and New York, 1990.